Key Threats to Digital Trade 2025

Asia-Pacific

This accompanies CCIA's annual National Trade Estimate Report filing. Information and data is current as of October 30, 2025. For more, visit: digitaltradebarriers.ccianet.org.

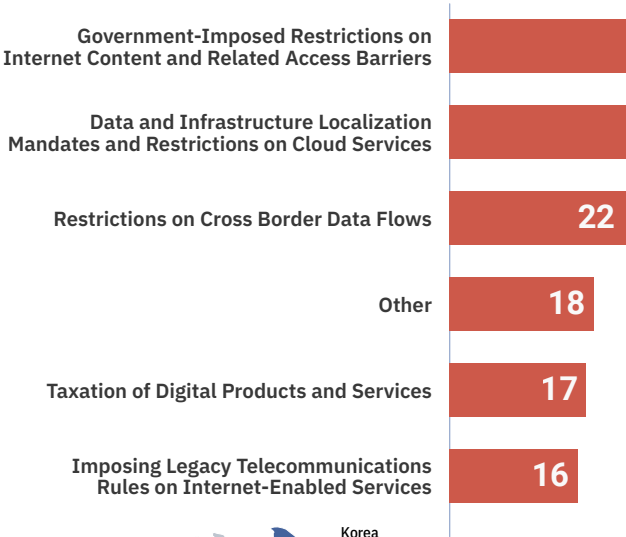
The United States has enjoyed strong diplomatic and economic relationships with the countries in the Asia-Pacific region for decades. Consumers in the United States import billions of dollars of goods and services from firms in the Asia-Pacific region annually as well.

This region includes analysis of policies in Australia, Bangladesh, Cambodia, China, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, Nepal, New Zealand, Pakistan, Papua New Guinea, Philippines, Singapore, Sri Lanka, Taiwan, Thailand, and Vietnam.

Services drive the benefits for U.S. exports in this mutually beneficial relationship, as are digital services. The U.S. generated **$160.4 billion in exports of digitally enabled services** to the region in 2024, bringing numerous positive externalities for business operations and consumers in the region, as well as a **trade surplus of $54 billion** in the sector.

The United States has formalized its trading partnership and economic cooperation with countries in the region in several fora, including the Indo-Pacific Economic Framework, the Asia-Pacific Economic Cooperation, and bilateral treaties.

Key Threats to the U.S.-Asia-Pacific trading relationship in 2025



CCIA identified

248

digital trade barriers in the Asia & Pacific region

174 policies enacted

74 policies in development

Digital Trade Barrier Trends for Asia-Pacific in 2025

Asymmetric Platform Regulation

Australia:

- Australia is exploring a potential **DMA-inspired regulatory framework for digital platforms**, targeting practices such as self-preferencing, tying, switching barriers, and data-related conduct. Potential legislation would impose DMA-style rules likely to raise compliance costs, deter investment, and disproportionately affect U.S. firms, reducing digital services investment by 17.4 percent and GDP by up to A$21.1 billion.
- Proposed **reforms to the Payments Act** would give Australia's central bank broad authority to oversee digital payment providers, establishing ministerial power to designate services deemed of "national significance" for additional regulatory oversight.

India:

- India is advancing DMA-style ex ante rules through proposals for a **Digital Competition Act** targeting "systemically important digital intermediaries," with obligations on anti-steering, platform neutrality, data use, ranking, and advertising that would predominantly affect U.S. firms. Although a 2024 draft **Digital Competition Bill** was later withdrawn pending a market study, the trajectory signals continued regulatory pressure that could disadvantage U.S. providers.

Japan:

- The **Act on Improving Transparency and Fairness of Digital Platforms** establishes transparency obligations for large online platforms designated as "Specified Digital Platform Providers." The law requires detailed disclosure of ranking criteria, data use, and contractual terms, along with annual reporting and potential oversight or enforcement. While intended to promote fair competition, implementation has disproportionately burdened U.S. firms through prescriptive reporting and opaque evaluations that exceed the law's stated "minimum necessary" standard. In July 2022, METI extended the TFDPA to cover the digital advertising sector, setting thresholds that clearly target major U.S. platforms. A February 2024 compliance review reinforced this focus, urging U.S. firms to modify operations under threat of ministerial action, illustrating the Act's expanding scope and discriminatory impact on foreign providers.
- The **Act on Promotion of Competition for Specified Software Used in Smartphones** establishes an ex ante regulatory regime for mobile ecosystem competition, closely modeled on the EU's Digital Markets Act. Only two U.S. firms are designated under the law, explicitly noting that no Japanese or third-country competitors meet the thresholds, reflecting a narrowly defined market intended to capture specific U.S. companies. The SSCPA prohibits 13 types of conduct, including tying, self-preferencing, and restrictions on interoperability or default settings, while allowing limited defenses. These presumptions risk penalizing practices that often enhance consumer welfare and innovation, imposing heavy compliance costs on U.S. firms. Moreover, Japan's decision to target U.S. suppliers while exempting domestic players with comparable market structures raises concerns about discriminatory treatment inconsistent with Japan's WTO commitments on national treatment and most-favored-nation obligations.

Korea:

- The proposed **Online Platform Monopoly Regulation Act** would impose sweeping restrictions on online service providers that meet arbitrary thresholds and ban self-preferencing, tie-in sales, and could mandate data sharing, creating risks for trade secrets and raising questions about Korea's WTO and KORUS obligations. Although some Korean firms are included, the thresholds disproportionately target U.S. platforms while exempting most domestic and non-market economy competitors. Following engagement with U.S. officials, the Korean government suspended the proposal indefinitely, but has not ruled out reintroduction. Korea is also

pursuing a related "**Platform Transaction Fairness" bill** which applies to intermediation services such as app stores, e-commerce platforms, and booking platforms. The proposal targets firms exceeding KRW 100 billion in brokerage fees or KRW 1 trillion in domestic sales, effectively capturing major U.S. platforms. It mandates standardized contracts, advance notice for contract changes, and impractically short payment deadlines, while imposing additional restrictions on companies deemed to hold a "superior bargaining position." These provisions mirror the EU's DMA-style obligations, limiting flexibility and competitiveness.

Thailand:

- The **Royal Decree on Digital Platform Services (B.E. 2565)** requires large-scale services to notify the government, appoint local representatives with unlimited liability, and implement mandatory risk management systems, with the Electronic Transactions Development Agency (ETDA) holding broad authority to impose future requirements.
- The government is pursuing new legislation, such as the previously drafted **Platform Economy Act (PEA)**, to supersede the Royal Decree, and the Trade Competition Commission of Thailand (TCCT) released draft **Guidelines on the Consideration of Unfair Trade Practices... in Multi-Sided Platform Businesses**, signaling a more interventionist antitrust posture.
- Furthermore, the Ministry of Digital Economy and Society (MDES) is considering new **OTT regulation** aimed at imposing tax obligations on international digital platforms under the guise of supporting local SMEs and combating "monopolization."

Vietnam:

- Vietnam has proposed a new **Law on Digital Transformation (Digital Transformation Law)** that is expected to negatively and disproportionately impact U.S. technology companies by imposing extensive ex-ante obligations and prohibitions, modeled on the EU's Digital Markets Act, on "very large-scale digital platforms" (VLDPs). This law would likely designate primarily U.S. firms and also includes provisions directing state entities to **prioritize procurement of digital products and services technologically mastered in Vietnam**, creating a direct market access barrier for foreign providers.

Barriers to the Deployment and Operation of Network Infrastructure

India:

- **Rules for satellite operators under the GMPCS license** impose extensive localization and security mandates, including domestic data centers or Points of Presence, local DNS resolution, and a ban on transferring or decrypting telecom data abroad. Operators must also enable emergency shutoffs, track user locations, and source 20% of ground equipment from Indian manufacturers within five years. These measures create significant barriers for foreign satellite providers, favoring domestic firms, raising entry costs, and introducing discriminatory local content and operational restrictions.

Indonesia:

- Indonesia's **subsea cable regime** imposes significant barriers to foreign infrastructure investment through restrictive routing, licensing, and partnership requirements. The decree mandates that all subsea cables follow a limited number of prescribed routes and landing points, despite over half of existing cables lying outside these corridors, and provides no clear process for approving new routes. Conflicting ministerial interpretations of landing sites and overlapping license requirements create further delays and uncertainty. Foreign cable operators are also required to partner with a local network operator holding at least a 5% consortium stake and five years of operating experience, even when cables only transit Indonesian waters.

- **Korea:**
  - The **Telecommunications Business Act** prohibits foreign operators, including satellite service providers, from directly offering telecommunications services in the country. Instead, they must contract with a domestic operator through a cross-border supply agreement approved by the Minister of Science and ICT. This requirement effectively bars independent market entry by foreign firms, forcing reliance on local partners and granting competitive advantages to domestic incumbents.

- **Malaysia:**
  - In November 2020, Malaysia revoked a 2019 exemption allowing non-Malaysian ships to conduct submarine cable repairs in its waters, reinstating restrictive **cabotage rules** under the Merchant Shipping Ordinance 1952. This reversal created significant delays, costs, and logistical challenges for global operators, particularly U.S. firms that maintain subsea infrastructure critical to global internet traffic. While the exemption was reinstated on June 2, 2024, the lack of permanence and the government's history of abrupt policy reversals continue to undermine investor confidence in Malaysia's digital infrastructure sector.

- **Philippines:**
  - The Philippines has imposed steep **duties on foreign subsea cable repair and installation ships** by classifying them as permanent imports, leading to multimillion-dollar costs and deterring investment in undersea cable projects. At the same time, spectrum allocation remains opaque, with no competitive auctions and a discretionary, nontransparent process that allows regulators to favor certain applicants, undermining fair competition in the telecom sector.

Customs-Related Restrictions and Import Barriers for Goods

- **India:**
  - Since August 2023, the government has imposed **import authorization requirements for laptops, servers, and tablets** under the Import Management System and is considering annual quotas that could disrupt supply chains and raise WTO compliance concerns. Additional mandates, including **Bureau of Indian Standards certification and MeitY approvals for AI and data center equipment**, have extended import timelines to six to eight months, slowing the deployment of advanced technologies. Meanwhile, the rapid expansion of **Quality Control Orders** across the electronics supply chain, rising from 88 in 2019 to over 700 by 2024, has introduced sweeping, protectionist compliance burdens that delay production and increase costs.

- **Indonesia:**
  - Indonesia **reclassifies covered ICT goods**, such as printers, data center equipment, routers, switches, servers, and optical components, into dutiable HS codes to increase tariff revenue, despite committing to duty-free treatment for five ITA categories. Moreover, **Ministry of Trade Regulation No. 31/2023**, which prohibits foreign merchants from selling goods under $100 to Indonesian consumers via online marketplaces and requires foreign e-commerce platforms to obtain Ministry of Trade permits, appoint local representatives, and separate manufacturing from marketplace operations, measures that directly hinder U.S. firms' access to Indonesia's e-commerce market. In addition, the **Ministry of Trade's Regulation No. 20/2021** maintains costly pre-shipment inspection requirements for imported ICT equipment, such as servers and cooling systems, adding up to $1,600 per shipment and creating administrative uncertainty due to opaque exemption procedures. Collectively, these tariff, e-commerce, and import measures significantly raise costs, restrict competition, and contravene Indonesia's WTO obligations.

- **Vietnam:**
  - The **Government Cipher Committee (GCC)** imposes onerous and inconsistently applied licensing requirements, specifically the **Cryptography Trading License** and **Cryptography Import License**, on any imported IT product with cryptographic functionality, causing up to six-month delays and restricting foreign firms from obtaining essential hardware.
  - Further regulatory uncertainty stems from the lack of an enforcement mechanism for the **Circular 23/2022/TT-BQP of Ministry of Defense** on cryptographic certification and a draft revised **Law on Tax Administration** that imposes uncertain extraterritorial tax declaration responsibilities on cross-border e-commerce platforms.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

- **Australia:**
  - The 2019 **Hosting Strategy** imposes ownership, control, and operational conditions on hosting and cloud providers. These rules effectively mandate data localization, residency, and personnel requirements for protected-level and whole-of-government data.
- **Bangladesh:**
  - The 2025 **Personal Data Protection Ordinance** and the **National Data Governance Ordinance** introduced criminal liability, extraterritorial provisions, and localization requirements for certain restricted data. The laws allow cross-border transfers only under limited conditions to jurisdictions deemed adequate, effectively compelling foreign providers to establish local data infrastructure.
- **Cambodia:**
  - The **2022–2035 Digital Policy Agenda** includes strict data localization and sovereignty mandates requiring confidential data to be stored or processed on in-country infrastructure operated by government-approved providers. While intended to protect national interests, these requirements effectively block the use of global cloud services.
- **China:**
  - China effectively **blocks foreign cloud service providers** from direct market participation by imposing licensing requirements and declining to grant licenses, forcing U.S. CSPs to operate only through franchise models. This approach, which likely violates China's WTO commitments on computer services, prevents fair competition and limits U.S. exporters from accessing one of the world's largest cloud markets.
  - The **Telecommunications Regulations**, **Classification Catalogue of Telecommunications Services**, and the **Negative List for Foreign Investment** jointly bar foreign CSP participation in key sectors.
  - China **restricts the use of foreign cloud services in sensitive industries** like financial services and smart vehicles, prohibiting international firms from using global public cloud infrastructure.
- **India:**
  - The 2020 expansion of **local content requirements** to software and services procurement mandates that suppliers meet 50% and 20% domestic content thresholds for Class I and Class II status, respectively, without a clear definition of "local content." Subsequent 2024 revisions tightened compliance by excluding imported components and services, increasing uncertainty for foreign cloud and software providers. These rules impose heavy documentation burdens, disregard non-tangible local contributions such as workforce training and infrastructure investment, and effectively disadvantage U.S. firms by conditioning market access on arbitrary localization metrics.

- The 2022 cybersecurity directions under **Section 70B of the IT Act** require cloud and VPN providers to log user activity and share personal information with authorities on demand. These surveillance mandates prompted many providers to exit the market and led to the blocking of 39 VPNs by 2024, creating an inhospitable environment for privacy-preserving services.
- The **Mandatory Testing and Certification Framework** has been expanded to include cloud software such as hypervisors, extending telecom equipment testing requirements to virtualized environments. This shift forces global providers to conduct local testing and potentially disclose proprietary information, duplicating international cybersecurity certifications and imposing costly, trade-restrictive burdens.
- The **2025 Securities and Exchange Board circular on digital accessibility** requires financial institutions' cloud and technology providers to obtain accreditation and undergo intrusive audits by the Ministry of Electronics and IT. The rules mandate data localization, government empanelment, and regulator access to infrastructure, effectively forcing foreign providers to rebuild operations in India.

Indonesia:

- **GR 71** retains localization mandates by requiring public sector electronic system operators to store data within the state-run National Government Data Center, while allowing limited flexibility for private operators to store data abroad.
- **GR 80** and **TR 31 on E-Commerce** prohibit offshore transfers of personal data without government approval and mandate that platforms promote domestic products, appoint local representatives, and share corporate data with authorities.
- Multiple overlapping **regulations restrict cloud use in financial services** by requiring data residency, regulator approvals for offshore processing, and AI models that prove data storage in Indonesia, effectively blocking many cross-border services. Bank of Indonesia and OJK rules treat cloud as high risk, mandate lengthy prior approvals, restrict outsourcing to "support work," and require domestic processing for key payments, creating discriminatory barriers that raise costs and exclude U.S. providers from competing on equal terms.
- **Decree No. 519/2024 on National Data Center Ecosystem Certification** requires public cloud providers to obtain local Indonesian National Standard certifications, even when equivalent ISO certifications are held internationally.
- The **Draft Cybersecurity Bill** would introduce fragmented oversight among multiple agencies, overlapping authorities, and expansive certification and localization mandates for cloud and data center operators.

Japan:

- The 2022 **Economic Security Promotion Act** empowers the government to strengthen control over critical infrastructure such as AI and cloud computing through targeted subsidies and supply chain measures. Under this framework, the government has provided substantial funding exclusively to domestic firms to develop "sovereign cloud" and AI supercomputing capabilities, effectively excluding U.S. cloud providers from Japan's most strategic AI initiatives. The 2025 **Act on the Protection and Utilization of Important Economic Security Information** established a security clearance system that mandates outdated, physical-only security measures for handling sensitive data. These requirements, along with Japan's **broader information security guidelines**, bar the use of modern cloud-based architectures and restrict U.S. hyperscalers from participating in public sector and defense projects.

Korea:

- The **Cloud Security Assurance Program (CSAP)** effectively excludes foreign cloud service providers from the public sector market. The program mandates physical separation of government data, use of domestic encryption algorithms, rejection of international certifications such as Common Criteria, and requirements that

data and personnel remain in Korea. These rules have prevented U.S. providers from qualifying for medium- and high-tier certifications that dominate the market, despite Korea's WTO and KORUS obligations prohibiting discriminatory technical barriers. Although revisions in 2023 allowed limited access for low-tier data through logical separation, core restrictions remain. Moreover, CSAP-like controls are expanding into sectors such as healthcare and education, where compliance is de facto mandatory through reimbursement and accreditation incentives.

- The **Industrial Technology Protection Act**, implemented to prevent leakage of sensitive technologies, has become a major barrier to foreign cloud service providers. The Act allows the government to designate "national core technologies" and restrict their export, foreign investment, and related data handling. Under this framework, the government prohibits the use of foreign cloud providers for workloads involving designated technologies, citing data security concerns. This effectively blocks Korean firms and research institutions from using global cloud infrastructure for advanced or high-performance workloads, compelling reliance on domestic providers regardless of capability or cost. The restriction discriminates against U.S. suppliers, limits innovation, and undermines Korea's obligations under WTO and KORUS commitments on market access and non-discriminatory treatment.
- The **National AI Initiative** aims to develop a domestic large language model and establish a National AI Computing Center forming the core of the country's AI infrastructure. However, the Request for Proposal included a "domestic companies only" clause, excluding U.S. cloud service providers from bidding on projects worth an estimated KRW 1.5 trillion (USD 1.1 billion). This abrupt, non-transparent restriction contradicts earlier signals of open competition and has raised serious concerns among U.S. firms that had invested heavily in local infrastructure. By denying foreign participation in one of Korea's most significant AI initiatives, the measure undermines fair procurement principles and appears inconsistent with Korea's WTO and KORUS government procurement commitments.

Malaysia:

- In October 2025, the State of Selangor introduced a **30% local content target for data center components**, including servers, memory, storage, and networking, to be sourced from domestic suppliers. The requirement, lacking clear enforcement mechanisms, could be tied to local permits and utility access, effectively coercing compliance. Similar measures are reportedly under consideration in Johor and at the federal level.
- In October 2025, Malaysia announced a **Sovereign AI Strategy** which establishes restrictive requirements for compute infrastructure, data residency, and certification for high-sensitivity government AI workloads. The plan prioritizes government-owned compute and cloud systems, potentially excluding foreign providers from critical national AI projects. However, the recent **U.S.-Malaysia Reciprocal Trade Agreement (Oct. 2025)** explicitly prohibits Malaysia from discriminating against U.S. digital services or imposing conditions that require U.S. firms to purchase, utilize, or accord a preference to a particular technology, while also committing Malaysia to ensuring cross-border data transfers for business conduct.

Nepal:

- The proposed **Information Technology and Cyber Security Bill 2080** would establish broad licensing and data localization requirements for digital infrastructure providers. The bill mandates that data centers and cloud service providers obtain annually renewable licenses and requires health and financial institutions to store all data domestically.

Philippines:

- The Philippines restricts foreign access to its cloud market through **domestic partnership requirements**, burdensome **SEC licensing** for public sector providers, and agency **mandates to use their GovCloud system**. Proposed data localization policies and broad regulatory powers under new laws risk imposing local data storage obligations and discriminatory rules against foreign firms, potentially undermining recent liberalization efforts and favoring large Chinese cloud providers.

Singapore:

- An amendment to the **2018 Cybersecurity Bill** was passed to expand reporting obligations and penalties to cover **Foundational Digital Infrastructure** providers, including cloud computing providers and data center facility services, even those located wholly overseas, imposing extra-territorial compliance burdens.

Sri Lanka:

- Sri Lanka's enacted but not-yet-operationalized data protection law, modeled after the EU GDPR, includes a **Section 26** that creates significant barriers to using cloud services located outside the country, favoring domestic data centers. This provision will complicate routine digital operations for Sri Lankan entities by requiring complex legal reviews and approvals for cross-border data processing, disproportionately burdening startups and MSMEs. Furthermore, the current language will make it virtually impossible for government entities to use global cloud services, hindering public sector digital transformation.

Taiwan:

- Financial institutions must follow the **Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation** to use cloud services, which, despite recent simplification efforts, involves a burdensome approval process that discourages cloud adoption and limits market access for U.S. providers.
- Regulators across sectors, including finance and healthcare, have expressed a strong preference for data localization, creating a *de facto* requirement that material customer data and medical data be stored in Taiwan, with vague and burdensome exemption processes.
- A September 2023 draft amendment to the **Cybersecurity Management Act (CSMA)** would direct sectoral regulators to establish rules for labeling critical infrastructure providers, introducing further regulatory uncertainty due to an unclear definition of "critical fields."

Thailand:

- Thailand's "Go Cloud First" policy, detailed in the draft **Government Cloud Usage Guidelines** and **Cloud Data Classification Guidelines**, signals an intent to increase cloud adoption but imposes significant data residency requirements, mandating that most government and regulated data be stored within the country. These guidelines, reinforced by the **National Cybersecurity Agency's Cloud Security Guidelines**, create market access barriers for U.S. cloud providers by effectively excluding cross-border services from public sector projects and explicitly reserving the top two tiers of government data (Secret and Top Secret) for state-owned enterprises.

United Arab Emirates (UAE):

- The UAE Cybersecurity Council mandates that federal and Emirate-level data workloads, along with data for financial services and healthcare, must be **hosted on servers within the UAE**.
- The government imposes strict sovereignty controls, requiring cloud services for the public sector and regulated industries to be solely subject to **UAE law**, not foreign jurisdiction, and to **physically localize** data centers and all associated operations and personnel.

- The **National Cloud Security Policy** formalizes this by requiring Secret and Top Secret data to be stored in fully sovereign infrastructure under exclusive UAE jurisdiction, though it offers clearer compliance pathways for foreign providers willing to localize.

- **Vietnam:**
  - Vietnam maintains extensive data localization and local presence mandates through the **Law on Cybersecurity**, detailed in **Decree No. 53/2022/ND-CP**, which requires domestic and foreign-invested firms to store copies of Vietnamese user data on domestic servers and can mandate localization for foreign firms whose services are used in violation of the law.
  - The newly enacted **Law on Personal Data Protection (Law No. 91/2025/QH15)** and the forthcoming **Personal Data Protection Decree** introduce stringent and burdensome cross-border data transfer restrictions, including mandatory **Overseas Transfer Impact Assessments** and extensive record-keeping, creating significant barriers to entry for foreign digital and AI-driven services.
  - The newly enacted **Law on Data (No. 60/2024/QH15)** introduces sweeping restrictions on "important" and "core" data, requiring burdensome preapproval for transfer abroad, which acts as a broad data localization obligation and disadvantages foreign cloud suppliers.
  - Finally, while the revised **Telecom Law** and **Decree No. 163/2024/ND-CP** liberalize some cross-border services, they still impose new compliance burdens, including mandatory notifications and the requirement that offshore cloud and data center providers store government data **exclusively in Vietnam**, effectively mandating local facilities.

Discriminatory Local Content Quotas and Audiovisual Service Mandates

- **Australia**:
  - The Australian government is considering **local content quotas and mandatory spending on streaming services**. A proposal requiring platforms to allocate 10–20% of local revenues or up to 20% of drama expenditures to Australian programs would create significant compliance burdens and conflict with Australia's AUSFTA obligations.

- **Korea:**
  - A proposed **amendment to the Framework Act on Broadcasting and Communications Development** that would require "value-added telecommunications providers" exceeding certain traffic thresholds to contribute 1% of their revenue to the Broadcasting and Communications Development Fund. While the fund supports domestic broadcasting and content development, foreign providers would be obligated to contribute without being eligible to benefit, creating a discriminatory funding scheme.

Forced Revenue Transfers for Digital News

- **Australia:**
  - The 2021 **News Media and Digital Platforms Mandatory Bargaining Code** requires designated platforms to negotiate payments with news publishers and, if necessary, enter compulsory arbitration. Only two U.S. companies have been targeted, raising procedural, trade, and IP concerns. The 2024 **News Bargaining Incentive**, a tax applying only to large foreign platforms, reinforces revenue transfers to local media and raises concerns of discrimination under trade commitments.

- **Indonesia:**
  - The 2024 **Presidential Regulation on Digital Platform Payments to News** mandates that digital platforms hosting Indonesian news content compensate local publishers through paid licenses, profit sharing, or other forms of cooperation. The measure, overseen by a committee dominated by domestic media interests, effectively targets U.S. platforms, introduces conflicts of interest in dispute resolution, and grants authorities broad discretion over platform operations.

- **Malaysia:**
  - A proposed **news remuneration framework** modeled on those in Australia and Canada would impose mandatory payments or revenue-sharing arrangements with news publishers. While the government has since shifted toward self-regulation through the Malaysia Media Council and created a public media fund, the MCMC's ongoing exploration of platform payment schemes raises market access concerns.

- **New Zealand:**
  - The **Fair Digital News Bargaining Bill**, introduced in 2023, would compel designated digital platforms to compensate news businesses for carrying or linking to news content, with the government estimating annual transfers of NZD 40–60 million from affected platforms—largely U.S. firms—to local media organizations. The bill allows news publishers to apply directly for a platform's designation, obliging it to enter mandatory bargaining even after voluntary agreements. It also introduces obligations for data sharing and cooperation with foreign regulators, raising operational and privacy concerns. While the government has since paused the bill, citing readiness issues, the proposal remains a significant potential barrier to U.S. firms.

- **Taiwan:**
  - Legislators in Taiwan have introduced proposals to the Legislative Yuan to establish a **mandatory news bargaining code** that would compel digital service providers to make revenue transfers to local news businesses. This legislative initiative is a discriminatory and trade-distortive framework, as it would impose targeted costs on foreign digital services and ignore the substantial voluntary investments already made by platforms to support Taiwan's news ecosystem.

Government-Imposed Content Restrictions and Related Access Barriers

- **Australia:**
  - 2019 amendments to the **Criminal Code** imposed new penalties on internet and hosting services that fail to quickly remove or report "abhorrent violent material." The law applies broadly to social media platforms, streaming services, and hosting providers, including U.S. firms, and was advanced without proper consultation or accounting for different business models and technical capabilities.
  - The 2021 **Online Safety Act** gives the eSafety Commissioner sweeping powers to order the removal of harmful content and to require eight online industry sectors to develop co-regulatory codes. Industry has voiced concern over vague definitions of "harm," disproportionate penalties, and discretionary enforcement, which risk forcing rapid content moderation under unclear standard.
  - The 2024 **Social Media Minimum Age Act** sets a mandatory minimum age of 16 for accounts on certain social media platforms, with no parental override. The measure disproportionately targets U.S. technology companies, disregards existing industry investments in age assurance solutions, and imposes requirements misaligned with current technologies.
  - A **proposal requiring internet companies to proactively take down scams** or face major fines would create mandatory obligations for proactive monitoring, significantly increasing operational costs for companies.

- Australia has failed to fully implement its AUSFTA obligation to provide **liability limitations for online service providers**, narrowing protections to "carriage" service providers rather than all online services. This violates Article 17.11.29 of AUSFTA, leaving U.S. digital service exporters legally vulnerable. Although authorities have long acknowledged this gap, recent copyright amendments expanded protections to some public bodies but excluded commercial platforms, disadvantaging U.S. firms and discouraging investment.

Bangladesh:

- The government has **blocked access to major social media and messaging platforms** during political unrest. These measures were accompanied by threats of further regulatory measures, such as data localization.
- The **Information and Communication Technology Act of 2006** grants the government sweeping authority to access and intercept data, block transmissions, and censor online communications. These powers have been used to restrict data services during politically sensitive events.
- The **Cyber Security Act of 2023** and the recently introduced **Cyber Security Ordinance** criminalize broad categories of online speech and empower the government to block or remove content.

Cambodia:

- **Censorship and mandated internet filtering** persist, with independent outlets frequently blocked during politically sensitive periods.
- The **National Internet Gateway** centralizes internet traffic through a government-appointed operator and requires businesses to use Cambodia's national domain. This system raises significant risks of content blocking and discriminatory treatment of foreign digital services.
- The draft **Cybercrime Bill** would impose intermediary liability, expand data localization mandates, and grant the government powers to take control of private operating systems during security incidents.

China:

- China maintains sweeping state control over online expression. The **2022 Provisions on Internet Post Comments** require platforms to verify user identities, pre-screen and monitor comments in real time, and report "illegal" or "negative" information to authorities. Complementary **2022 Social Media Monitoring Rules** mandate real-time monitoring of user activity, including "likes," while the **2023 Cyberbullying Guidelines** would criminalize vague categories of speech such as "rumor-spreading," obliging platforms to proactively detect and remove content or face penalties. Real-name disclosure rules for influencers intensify privacy risks, and the **2024 National Network Identity Proposal** would create a unified national digital ID to consolidate state tracking. Meanwhile, the **2024 Regulations on Online Violence** require the removal of politically sensitive material and enforce adherence to "correct political direction," granting authorities broad discretionary power to suppress speech.

Hong Kong

- The 2020 **National Security Law** and subsequent 2021 **Personal Data (Privacy) (Amendment) Ordinance** grant authorities sweeping powers to compel content removals, block websites, and demand platform compliance beyond Hong Kong's borders, undermining online freedom and creating barriers to digital trade. The 2024 **Safeguarding National Security Ordinance** further expands these powers by criminalizing broad categories of speech and online activity, introducing severe penalties that threaten freedom of expression and heighten operational risks for U.S. digital service providers.

India:

- The ongoing use of **internet shutdowns** continues to impose severe economic and human rights costs, disproportionately affecting both users and digital service providers. India has remained the global leader in shutdowns for six consecutive years, and authorities continue to invoke broad powers under the Telegraph Act of 1885 and other laws to restrict connectivity, often bypassing safeguards meant to limit such orders. The continued renewal of temporary suspension orders under the 2024 Rules perpetuates uncertainty, undermines digital trade, and weakens confidence in India's commitment to maintaining an open and reliable internet environment.
- The **amended IT Rules** impose sweeping obligations on online intermediaries to prevent and remove broadly defined categories of content deemed harmful or against national interests, while mandating localization, traceability, and rapid takedown measures that risk undermining encryption, privacy, and free expression. The establishment of Grievance Appellate Committees, government fact-checking bodies, and the Sahyog portal, used to expedite blocking and data disclosure orders, has further expanded state control over digital content and eroded intermediary protections.

Indonesia:

- Recurring **internet shutdowns and excessive content takedown requests** have caused significant financial losses for U.S. firms and raised concerns over online freedom of expression. Between 2019 and 2021, the U.S. International Trade Commission estimated $82.2 million in economic losses from shutdowns, while Meta reported 47 million content restrictions in late 2023.
- **Ministerial Regulation 5/2020** mandates registration, local representation, and system access for all domestic and foreign digital service providers. The opaque and burdensome framework requires rapid compliance with government takedown and data access orders, risking exposure of user data and creating significant operational uncertainty for U.S. firms, as seen in multiple service suspensions for non-registration.
- **Government Regulation 43/2023** introduces fines of up to US$30,000 per non-compliant URL, compounding compliance risks for foreign online service providers. Vague definitions, limited transparency in appeals, and unrealistic takedown timelines heighten the risk of arbitrary enforcement.
- The **revised Criminal Code** expands corporate liability and criminal penalties for online content deemed blasphemous, insulting to officials, or contrary to national ideology. The law's broad and ambiguous provisions expose digital platforms and their employees to prosecution for user-generated content, creating major compliance uncertainty and threatening free expression.
- **Decree 172** establishes a centralized system for issuing takedown orders and fines to enforce content moderation rules. The system lacks transparency, clear appeal procedures, and technical guidelines, raising concerns over due process, data security, and arbitrary application once fully operational.
- **Government Regulation No. 17/2025** on Child Safety Online introduces vague risk classifications and access bans for minors, mandating strict verification and consent mechanisms. Its overbroad scope and unclear implementation standards create significant compliance burdens for global platforms, risking over-removal of lawful content and limiting youth access to beneficial online services.

Japan:

- **Act No. 137** conditionally shields internet and telecommunications providers from liability while allowing rights-holders to request disclosure of user information in online infringement cases. Amendments in 2021 created a streamlined "Sender Information Disclosure Procedure," which rights-holders have since used to target U.S.-based infrastructure providers, exposing them to disproportionate litigation risks. Additionally, the **Corporate Law** requirement for foreign firms to register their U.S. entities locally heightens legal exposure.

Korea

- The **Network Act** and forthcoming proposals by the Korea Communications Commission collectively introduce major new barriers for cross-border digital services. The 2024 amendment to Article 44-7(5) requires providers operating domestic servers to monitor, block, and document "unlawful information," effectively creating a de facto data localization requirement and expanding liability risks for foreign suppliers. The KCC is also advancing further amendments that would mandate large online platforms to remove vaguely defined "false or manipulated information" or face investigations and fines of up to 4 percent of domestic sales. These proposals risk politicizing content moderation, compel over-censorship, and subject foreign platforms to discriminatory and burdensome compliance obligations inconsistent with Korea's KORUS and WTO commitments.

Malaysia:

- A **new social media licensing regime** and the **Online Safety Act 2025** significantly expand state powers over digital content and platform operations. These measures create broad liability risks and enable discretionary content takedown orders without judicial oversight, raising serious freedom of expression and rule-of-law concerns. For U.S. firms operating large platforms, compliance costs and legal risks are expected to rise sharply, incentivizing over-removal of lawful content.

Nepal:

- The **National Cyber Security Policy** proposes a government-controlled National Internet Gateway, modeled after Cambodia's system, to centralize and monitor all internet traffic entering and leaving the country. The gateway would enable state filtering and censorship of online content, effectively creating a government-owned intranet. This measure poses serious risks to internet openness, human rights, and business continuity for U.S. firms, as it would restrict competition, undermine cross-border service provision, and allow pervasive government surveillance.

- The **Social Media Directive** requires foreign platforms to register locally, appoint liaison officers, and implement complaint-handling and moderation systems. The Directive imposes extensive content moderation obligations without clear safe harbor provisions, exposing platforms to liability for user-generated content. These requirements risk creating a de facto local presence mandate for U.S. platforms, raising barriers to cross-border digital trade and restricting the ability of global firms to operate in Nepal. The **Social Media Act Bill** would codify many elements of the earlier Directive while significantly expanding government powers. The bill mandates registration for all social media platforms operating in Nepal, imposes strict moderation duties, and allows authorities to order the removal of vaguely defined "indecent" or "misleading" content. It also criminalizes online speech deemed defamatory or "malicious," with penalties of up to five years' imprisonment and fines up to 2.5 million NPR.

- **Nepal's E-Commerce Act 2081** establishes sweeping regulatory and jurisdictional powers over foreign digital service providers. The law requires local registration, licensing, and compliance with Nepali consumer protection, contract, and data privacy rules, while classifying global online platforms as intermediaries potentially liable for third-party conduct such as fraudulent listings or misleading advertisements. It also mandates extensive obligations for seller verification, payment transparency, and dispute resolution, with significant penalties for noncompliance.

- In September 2025, Nepal's government ordered the **blocking of 26 major social media platforms** that failed to register under its existing regime, triggering widespread protests and legal challenges that led to the order's withdrawal. The incident underscores the unpredictable and restrictive trajectory of Nepal's digital governance framework, which continues to pose systemic risks to freedom of expression and market access for U.S. firms. CCIA urges USTR to remain engaged and press for regulatory reforms ensuring transparent, proportionate, and non-discriminatory treatment of digital service providers in Nepal.

New Zealand:

- A proposed **Social Media (Age-Restricted Users) Bill** would require social media platforms to take reasonable steps to prevent users under 16 from creating accounts on government-designated age-restricted platforms. Noncompliance could result in civil penalties of up to NZD 2 million. The bill empowers the government to determine which platforms are covered, issue implementing regulations, and conduct a review after three years. While intended to protect minors online, the proposal could impose heavy compliance and administrative burdens on foreign platforms, including U.S. providers, by requiring costly age-verification systems and introducing new legal liabilities.

Pakistan:

- In 2025, Pakistan established the **Social Media Protection and Regulatory Authority (SMPRA)** with sweeping powers to regulate, fine, and block social media platforms, expanding censorship to content deemed false or critical of state institutions. Combined with frequent internet shutdowns and a new national firewall, these measures have caused major economic losses, estimated up to $1.6 billion, and raised serious concerns about censorship, human rights, and foreign investment.

Papua New Guinea:

- Papua New Guinea's 2025 **National Social Media Policy** requires users aged 14 and above to obtain a SevisPass digital ID to access major platforms and mandates local registration and compliance for social media companies. These measures, enforced by a new national e-Safety Directorate, could significantly raise operational costs for foreign platforms and restrict market access through stringent localization and verification requirements.

Philippines:

- The Philippines' 2023 **Internet Transactions Act** requires digital platforms to register with the Trade Ministry, verify merchant identities, and regularly submit merchant lists, with criminal penalties for noncompliance. These measures grant broad takedown powers to regulators and impose heavy compliance and privacy burdens on e-commerce platforms, potentially hindering digital trade and market participation.

Singapore:

- Singapore's digital environment is heavily regulated by several laws that grant the government broad content moderation powers, including the **Protection from Online Falsehoods and Manipulation Bill (POFMA)**, which requires platforms to remove or carry corrections for content deemed false or misleading, and the **Foreign Interference (Countermeasures) Act (FICA)**, which requires platforms to act against content covertly influenced by foreign actors.
- The **Online Safety (Miscellaneous Amendments) Bill** empowers the IMDA to regulate "egregious content" and compel online services to comply with Codes of Practice, while the **Online Criminal Harms Bill (OCH Bill)** gives authorities power to issue "Government Directions" to services to restrict online activity suspected of committing a crime.
- Additionally, the recently introduced **Online Safety (Relief and Accountability) Act (OSRA)** will create the **Online Safety Commission (OSC)** with powers to issue directives to online platforms for prompt content removal and to demand user identity information related to online harms like harassment and deepfakes.

Sri Lanka:

- The Sri Lankan **Online Safety Act**, certified in February 2024, is widely criticized for giving the yet-to-be-activated **Online Safety Commission** unchecked authority to determine what constitutes a "false statement," which is criminalized under the law. The Act's vague definitions, broad information-gathering powers, and provisions allowing the Commission to order the removal of "prohibited statements" pose a high risk of arbitrary enforcement and suppression of dissent, particularly against U.S. service providers.

Taiwan:

- The **Fraud Crime Harm Prevention Act** imposes serious, burdensome anti-fraud obligations on designated online advertising platforms, including stringent verification, disclosure, and content removal requirements, which may act as a non-tariff trade barrier.
- Taiwan's overall sectoral approach to intermediary liability systematically erodes safe harbor protections, effectively imposing strict liability on platforms for user-generated content, exemplified by the **Tobacco Hazards Prevention Act** improperly shifting legal responsibility from the content creator to the intermediary.

Thailand:

- Thailand maintains extensive government oversight of online content via the **Computer Crime Act**, which is leveraged by the **Anti-Fake News Center** to demand takedowns of content deemed "false and misleading" under a broad definition of "National Security."
- The **Cybersecurity Law** grants officials authority to "search and seize data and equipment" in national emergency cases, enabling government surveillance.
- The **Emergency Decree on Cybercrimes**, coming into effect in 2025, assigns liability to digital platforms for online scams if they fail to implement regulator-prescribed prevention measures, including removing fraud content within 24 hours of notification.

United Arab Emirates (UAE):

- The UAE maintains longstanding regulatory restrictions on unlicensed **Voice over Internet Protocol (VoIP)** services, selectively blocking the voice and video features of popular foreign platforms like WhatsApp and FaceTime, which protects the revenue of the state-licensed telecom duopoly and allows for government control over communications.
- The **2018 National Media Council Content Creators law** imposes onerous licensing requirements on a broad scope of social media influencers, including foreign residents and those with paid associations, which creates unnecessary friction and a potential selective enforcement mechanism inhibiting digital trade.

Vietnam:

- Vietnam's **Law on Cybersecurity** requires online services to monitor and remove vaguely defined "prohibited" content—including material critical of the government—within 24 hours of notification, and grants authorities the power to demand access termination and user information, often coupled with technical interventions like throttling.
- **Decree 71/2022/ND-CP** extends broadcast television regulations to cross-border video-on-demand services, requiring them to operate through domestically managed websites/IP addresses and limiting foreign-controlled advertising.
- **Decree No. 147/2024/ND-CP** imposes sweeping, onerous obligations on "Regulated Cross-Border Services" (platforms with over 100,000 monthly visits), including mandatory content takedowns, user data handover upon request, intrusive identity verification (mobile/national ID), and local contact point notification.

- The draft **Law on E-Commerce (2025 Draft E-Commerce Law)** would extend regulatory oversight to social-media commerce and affiliate marketing, mandating that foreign platforms establish a local entity, deposit funds, and comply with transparency rules.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Bangladesh:

- An **amendment to the Bangladesh Telecommunication Regulatory Act** would bring digital platforms under the telecom regulator's jurisdiction, while imposing vague takedown standards and weakening privacy safeguards.

India:

- India has proposed **bringing OTT and cloud providers under telecom-style licensing** and allowing selective blocking of services, raising major concerns about regulatory duplication, censorship, and harm to competition and innovation. The 2023 **Telecommunications Act** further broadened the definition of "telecommunication services" to include OTT, user-to-user communication, and cloud services, subjecting them to licensing, fees, and government control without equal access to public funding mechanisms. Subsequent **TRAI recommendations and Department of Telecommunications advisories** in 2024 and 2025 expanded these controls, including content removal orders and obligations tied to infrastructure, data access, and encryption mandates. Collectively, these measures create one of the most intrusive and burdensome licensing regimes for internet-enabled services globally, raising serious concerns about privacy, market access, and consistency with India's WTO GATS commitments. Complementing these measures, the withdrawn 2024 **Broadcasting Services (Regulation) Bill** sought to impose broadcast-style oversight on digital and social media platforms, requiring registration and content evaluation for "digital news broadcasters," while a proposed **CDN regulatory framework** would bring content delivery networks under telecom-style authorization and compel disclosure of confidential peering agreements.

Indonesia:

- The draft **Broadcasting Bill** seeks to extend traditional broadcasting rules to internet streaming platforms, bringing them under licensing, censorship, and state content oversight. As amended, the draft Bill would expand government control and impose stricter content standards, raising serious concerns for online service providers, freedom of expression, and the open internet.

Korea:

- Korea's amendments to the **Telecommunications Business Act** have expanded the Act's scope to impose network management responsibilities on value-added telecommunications service providers, including OTT platforms, despite their lack of control over network infrastructure. Moreover, multiple proposed bills would mandate that high-traffic platforms pay "legitimate" fees to ISPs, effectively codifying Korea's **"Sending Party Network Pays"** regime. This model, first introduced in 2016, has already resulted in some of the world's highest wholesale bandwidth costs, degraded network performance, and market distortions favoring domestic ISPs.

Malaysia:

- Amendments to the **Communications and Multimedia Act 1998** impose legacy telecom-style obligations on cloud service providers, including compliance with data access and interception requests, and contributions to the **Universal Service Provision Fund (USPF)**.

- The **Framework for Internet Safety** requires large social media and cloud providers to register, obtain a license, and comply with invasive obligations, such as warrantless data disclosure and government-directed content removal. While the Framework previously required a discriminatory 6% revenue contribution to the

USPF, the October 2025 **U.S.-Malaysia Reciprocal Trade Agreement** formally commits Malaysia to not imposing discriminatory digital services taxes or similar taxes on U.S. companies, thereby securing the removal of the levy, though the change still requires formal legislative implementation by the MCMC.

- **Nepal:**
  - In March 2022, Nepal amended its **National Broadcasting Rules** to require broadcast OTT, video-on-demand, and online television services to obtain licenses from the Ministry of Information and Communications before operating in Nepal. The amendments also obligate OTT providers to maintain local cache servers, store user data and program records for at least 60 days, and implement age-based content categorization. In April 2023, the Nepal Telecommunications Authority introduced a **draft OTT Regulatory Framework** extending licensing and registration requirements to voice, video, and messaging OTT services, mandating that providers establish a local branch or appoint an in-country intermediary.

Potential Challenges to the Development of AI

- **Australia:**
  - Proposed **mandatory guardrails on high-risk AI systems** would classify all general-purpose AI as high risk, creating significant compliance and disclosure burdens.

- **China:**
  - The **Interim Measures for the Management of Generative Artificial Intelligence Services** requires providers of generative AI systems to obtain licenses and register with regulators. Suppliers must use technical means to prevent and report illegal or false content, ensure training data complies with intellectual property and privacy rules, and align services with "socialist values." The rules also impose obligations to implement anti-addiction tools, privacy safeguards, complaint mechanisms, and competition restrictions, though the latter remain vaguely defined.
  - Thr **draft Guidelines for Standardizing the Artificial Intelligence Industry** would establish more than 50 national AI standards and participate in 20 international standards by 2026, signaling an effort to shape global AI norms around China-specific frameworks.
  - The **draft Cybersecurity Technology – Basic Security Requirements for Generative AI Service regulation** would require providers to implement security assessments, apply safeguards around training data, and limit harmful outputs to 5%. The mandatory sharing of sensitive training data and security information with Chinese authorities raises serious concerns about the protection of U.S. intellectual property and trade secrets.

- **Korea:**
  - The **AI Basic Act** introduces sweeping obligations on AI developers and deployers that create major barriers for cross-border AI service providers. The law's lack of clear differentiation between developers, deployers, and users exposes large U.S.-based AI firms to liability for downstream uses beyond their control, while compute-based thresholds for "high-performance" AI risk disproportionately targeting U.S. providers. Requirements for public disclosure of training data, model criteria, and AI-generated outputs threaten trade secrets and duplicate industry-led standards, increasing compliance costs and uncertainty. The mandate for foreign providers to appoint a domestic agent liable for violations functions as a de facto local presence requirement, inconsistent with KORUS Article 12.5, and intrusive fact-finding powers raise further enforcement risks.

- **Malaysia:**
  - A **proposed AI Bill** risks entrenching an "AI sovereignty" model that favors local AI systems. The launch of Malaysia's ILMU model in August 2025 and the Prime Minister's announcement of a "sovereign AI cloud" in the 2026 Budget signal a policy direction restricting public-sector use of global AI models. Such measures risk excluding U.S. AI providers from major government contracts, but the recent **U.S.-Malaysia Reciprocal Trade Agreement** bars discrimination against U.S. digital services and explicitly prohibits Malaysia from imposing conditions that require U.S. firms to 'purchase, utilize, or accord a preference to a particular technology'.

- **Vietnam:**
  - The draft **Digital Technology Industry Law (DTI Law)** includes technically impossible obligations, mandates monitoring of downstream AI use, prioritizes procurement of domestically produced technology, and gives regulators sweeping, vague oversight authority that risks subjective enforcement and censorship.
  - The standalone draft **Law on Artificial Intelligence (AI Law)** establishes a rigid, risk-based pre-market management approach that imposes resource-intensive requirements—including local establishment, detailed logging, and conformity assessments for high-risk systems—which are ill-suited for the fast-evolving technology and deter foreign developers.
  - The draft **Personal Data Protection Decree** contains restrictive AI-related provisions, such as mandating **consent as the sole legal basis for AI model training** and granting government agencies authority to **order the destruction of AI algorithms**, which is viewed as an extreme measure that undermines investor confidence.

Restrictions on Cross-Border Data Flows

- **Cambodia:**
  - The **draft Law on Personal Data Protection** includes high administrative fines of up to 10 percent of annual turnover, rigid compliance timelines, and a broad right to erasure, creating significant financial and legal risks for U.S. service providers. The law's elevated age of consent at 16 also diverges from global norms.

- **China:**
  - China maintains overlapping regulations that make data transfers prohibitively difficult. Barriers include **strict personal information transfer restrictions**, **forced joint ventures for foreign cloud providers**, **foreign investment limits**, and extensive censorship through the **Great Firewall**. Stringent cross-border data transfer rules under the **2019 Cybersecurity Law**, **2021 Data Security Law**, **2021 Personal Information Protection Law**, and subsequent implementing measures require categorizing data into vague sensitivity levels, mandatory security assessments, audits, and reporting, with some categories facing outright export bans.

- **India:**
  - The **Digital Personal Data Protection Act** introduced narrow consent-based grounds for data processing and enabled the government to prohibit data exports to unspecified jurisdictions without clear criteria or recourse mechanisms. The Act also permits the introduction of data localization mandates through other sectoral laws, creating significant uncertainty for cross-border data flows. In 2025, the government began developing **implementing rules** that would expand its authority to designate "significant data fiduciaries" and impose domestic storage obligations on select entities, while restricting international data transfers solely to destinations approved by the government. These rules risk creating a fragmented and protectionist data regime that diverges from global best practices.

Indonesia:

- Indonesia's **Personal Data Protection Law** establishes rules for data controllers and processors, including cross-border transfer limits to countries with "equivalent" data protection, though criteria remain undefined. While Indonesia and the United States announced a bilateral adequacy framework recognizing the U.S. as an equivalent jurisdiction in 2025, sector-specific localization mandates and pending revisions to GR 71/2019 could weaken its effectiveness.

Japan:

- Amendments to the **Telecommunications Business Act** expanded the coverage foreign suppliers of internet-based services, even those without a legal presence in Japan. The amendments require foreign OTT platforms, such as search, digital advertising, and communications services, to register locally, appoint a representative, and comply with domestic obligations under the TBA. In 2022, MIC further extended the law to impose privacy and data protection obligations on large platforms, including rules governing the use and transfer of third-party data such as cookies. Additional 2023 amendments mandate that telecommunications providers disclose extensive information to users regarding data transmission and processing. Collectively, these measures impose complex compliance requirements on U.S. and other foreign providers.

- Amendments to the **Act on the Protection of Personal Information** introduced stricter requirements on cross-border data transfers and privacy compliance. The revised framework mandates that companies either obtain explicit opt-in consent from users before transferring personal information overseas or demonstrate that the recipient operates under a recognized personal data protection regime. The amendments also tightened breach notification rules, enhanced data subject rights, and allowed for extraterritorial enforcement, bringing Japan's privacy regime closer to the GDPR but increasing operational burdens for U.S. firms. These heightened requirements have complicated data transfers and created potential conflicts with global business models.

Korea:

- The amended **Personal Information Protection Act** and associated enforcement practices impose disproportionate compliance burdens and risks on foreign service providers. The 2023 reforms unified cross-border data transfer obligations for both online and offline entities, maintaining stricter requirements for foreign transfers while applying lighter standards to domestic transfers—effectively privileging Korean over foreign suppliers without improving privacy outcomes. The amendments also introduced new rights to data portability and expanded the government's powers to levy fines of up to 3% of global revenue. Moreover, the PIPC's authority to suspend cross-border data flows based on generalized "risk" rather than concrete violations introduces legal uncertainty and could arbitrarily disrupt data transfers between Korean subsidiaries and their U.S. headquarters.

- The continued **prohibition on the export of map dat**a constitutes one of the world's most restrictive geospatial data regimes and a major market access barrier for foreign service providers. Foreign mapping and navigation platforms are effectively barred from exporting map data for processing abroad, while domestic competitors face no such restriction. Despite multiple applications from U.S. firms, the Korean government has consistently denied export approval, conditioning any potential authorization on blurring certain satellite imagery for purported security reasons—despite the same imagery being commercially available globally. This discriminatory policy prevents foreign firms from offering fully functional mapping services in Korea and distorts competition in favor of local providers.

- **Pakistan:**
  - Pakistan's draft **Personal Data Protection Bill**, last revised in early 2025, grants the government broad powers to restrict cross-border data transfers on vague grounds such as "public interest" or national security, effectively enabling data localization and creating major uncertainty for foreign firms. Combined with existing sectoral rules that already mandate local data storage, the proposed framework would severely limit the use of global cloud infrastructure and raise compliance costs for both domestic and international companies.

- **Taiwan:**
  - The initiative by Taiwan's Personal Data Protection Committee Preparatory Office to develop a unique, domestic set of **Standard Contractual Clauses (SCCs)** for cross-border data transfers raises serious concerns. By pursuing a bespoke framework incompatible with international standards, Taiwan risks creating a fragmented and legally uncertain environment, imposing significant compliance burdens and costly, duplicative contractual arrangements on multinational companies.

- **Thailand:**
  - Thailand's **Personal Data Protection Act (PDPA)**, which took effect on June 1, 2022, creates restrictions on cross-border data flows due to its broad **extraterritorial reach**. The law applies to entities outside of Thailand that process the personal data of Thai residents, creating potential liability and compliance burdens for U.S. online services even if they lack a physical business presence in the country.

Taxation of Digital Products and Services

- **Australia:**
  - The **Treasury Laws Amendment (GST Low Value Goods) Act 2017** requires foreign companies with over AU$75,000 in annual sales to Australian customers to register and remit GST on all imported goods, including low-value items. This policy creates a de facto market access barrier by shifting tax collection responsibilities to foreign firms.
  - The proposed rule **TR 2024 D1** would redefine software licensing arrangements so that software delivery, including downloads and cloud-based services, could be treated as royalty payments subject to withholding tax, departing from prior Australian practice and OECD norms.

- **India:**
  - India's **income tax framework** creates significant uncertainty regarding whether the provision of data center or digital services by an Indian entity to a foreign client constitutes a taxable presence for that foreign entity. Ambiguity in applying these concepts to modern service-based digital models exposes foreign firms to potential double taxation and heavy compliance burdens, even when transactions follow standard cost-plus arrangements.

- **Indonesia:**
  - **Regulation No. 17/PMK.010/2018** adds "software and other digital products transmitted electronically" to its tariff schedule, making it the only country to include electronically transmitted goods under customs law. While the rate is currently zero, this measure conflicts with Indonesia's WTO commitment to the moratorium on e-commerce duties. Under the July 2025 U.S.–Indonesia Reciprocal Trade Agreement Framework, Indonesia agreed to eliminate these tariff lines and support a permanent WTO moratorium, though full implementation will be key to restoring legal certainty for digital trade.

- The proposed **Electronic Transaction Tax** would treat foreign digital service providers with a "significant economic presence" as permanent establishments subject to domestic taxation. The measure departs from international tax norms, risks double taxation, and disproportionately targets non-Indonesian—particularly U.S.—companies.
- The **12% VAT on digital goods and services delivered via electronic systems** applies broadly to SaaS, streaming, advertising, and cloud services exceeding an annual threshold of IDR 600 million, imposing registration, tax ID validation, and reporting burdens on foreign providers
- **Minister of Finance Regulation No. 37/2025 on E-Commerce Income Tax** imposes a 0.5% final income tax on e-commerce transactions, collected by major online marketplaces from domestic sellers with annual revenues above Rp 500 million. Though temporarily postponed, the tax creates compliance burdens and risks double taxation.

Japan:

- Japan imposed new **obligations requiring certain online platforms to collect and remit consumption taxes** on behalf of non-Japanese businesses providing digital services to Japanese consumers, applying a transaction threshold of ¥5 billion (US$32.9 million). Japan is now considering expanding this regime to cover additional cross-border e-commerce transactions, which could exacerbate competitive disparities if the high threshold persists.

Nepal:

- Nepal's Finance Act for FY 2022/23 introduced a **2% DST** applying exclusively to non-resident companies providing digital services. The tax contradicts established international tax norms, risks double taxation, and places disproportionate administrative burdens on U.S. and other foreign firms required to register, remit, and report DST payments locally.

Pakistan:

- In 2025, Pakistan introduced a **DST** targeting offshore platforms with a "significant digital presence," but its enforcement was suspended by the Federal Board of Revenue, creating uncertainty about future implementation. Nonetheless, overlapping federal and provincial tax measures continue to apply extraterritorially to digital firms, expanding taxation to companies with only virtual operations in Pakistan.

Philippines:

- The Philippines imposes complex and burdensome tax procedures on non-resident service providers, requiring lengthy treaty-status approvals and unclear income tax rules that deviate from international norms. A new **12% VAT** on digital services further increases compliance risks, as forthcoming regulations may introduce onerous obligations for foreign digital providers similar to those already affecting income tax filings.

Sri Lanka:

- Sri Lanka has announced an **18% VAT** on digital services supplied by non-resident entities, scheduled to take effect in April 2026. This tax will apply to a wide range of digital services, and the draft implementation framework is creating legal uncertainty and administrative burden due to a lack of clarity on compliance and registration procedures, which was developed without adequate industry consultation.

Vietnam:

- Vietnam's **Tax Administration Law** (effective July 1, 2020), guided by **Circular 80**, imposes a discriminatory Foreign Contractor Tax (FCT) on gross revenues of foreign digital service and e-commerce suppliers lacking a permanent establishment. This tax creates a significant financial burden on U.S. commerce and is exacerbated

by **unclear and discriminatory administration of double tax relief applications**, where U.S. companies face long delays, onerous requests, and unjustified rejections that conflict with Vietnam's bilateral tax treaty obligations.

Threats to Encryption and Security of Devices

Australia:

- The **Telecommunications (Assistance and Access) Act 2018** grants Australian security and law enforcement agencies broad powers to compel technology companies to assist in accessing encrypted communications. While it formally prohibits introducing systemic vulnerabilities, the law allows the government to undermine encryption through other technical means with limited oversight.
- The **Critical Infrastructure Protection Bill 2022** expands the scope of critical infrastructure to include data storage and processing services and imposes extensive security and reporting obligations. It also grants the government sweeping powers to direct companies, install monitoring software, or take control of assets.

China:

- Amendments to the **Commercial Cryptography Administrative Regulations** weakened alignment with international standards and introduced opaque import and export control provisions that could amount to mandatory certification requirements.
- China's **Standardization Law** embeds security and technological requirements into market participation rules. Chinese cryptographic standards referenced in regulation mandate the use of domestically developed algorithms, excluding foreign companies from the standards-setting process.

Hong Kong

- The **Protection of Critical Infrastructure Act** designates "information technology and communications" as critical infrastructure and grants authorities sweeping investigatory powers, including the ability to access, modify, or install programs in private systems. The law's overly broad definitions and extraterritorial reach could subject a wide range of digital service providers, including foreign firms, to intrusive government control and compliance risks.

Korea:

- Amendments to **Korea's Broadcasting Communications Development Act, Telecommunications Business Act, and Network Act**, passed following a major data center fire, impose extensive data disclosure requirements on operators to promote infrastructure resiliency. These obligations compel companies to submit detailed information on data center operations, security systems, and risk management practices, exposing sensitive technical and commercial data to potential disclosure. Such requirements raise serious cybersecurity and confidentiality concerns, as they risk compromising trade secrets and weakening the overall security posture of both domestic and foreign service providers operating in Korea.

Malaysia:

- Recent amendments to the **Communications and Multimedia Act** grant law enforcement broad powers to access communications data and install interception devices without warrants. These provisions expose U.S. companies to severe compliance conflicts, as obeying Malaysian demands could violate U.S. data protection laws, while refusal risks fines up to RM 1 million or imprisonment. The warrantless entry clause for interception poses a critical cybersecurity threat.