KEY THREATS TO DIGITAL TRADE 2022

Asia & Pacific

This two-pager accompanies CCIA's annual National Trade Estimate Report filing. Information and data is current as of October 31, 2022. For the most recent dataset visit digitaltradebarriers.ccianet.org.

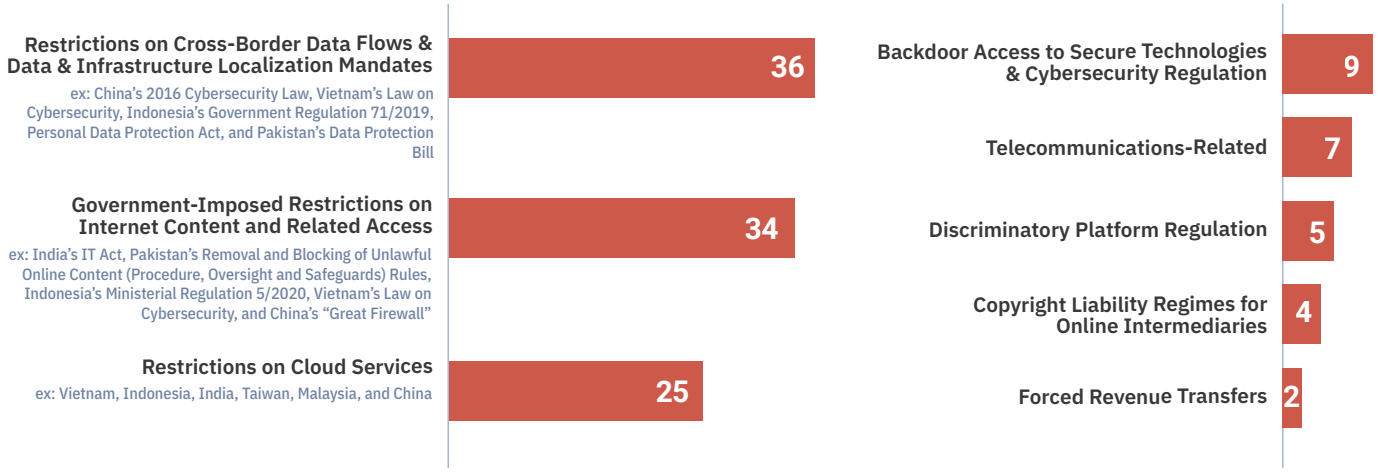
The United States has enjoyed strong diplomatic and economic relationships with the countries in the Asia and Pacific region for decades. Several countries in the region have served as key markets for U.S. companies such as Japan, Korea, India, Indonesia, Australia, New Zealand, and Singapore to name a few. Consumers in the United States import billions of dollars of goods and services from firms in the Asia and Pacific region annually as well.

This region includes analysis of policies in Australia, Bangladesh, Cambodia, China, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, New Zealand, Pakistan, the Philippines, Singapore, 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 **$164.5 billion in exports of digital services** to the region in 2021**,** bringing numerous positive externalities for business operations and consumers in the region and a **trade surplus of $63.9 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. As work is done to advance these initiatives, the United States should ensure partners do not restrict the ability of U.S. firms to enter or expand into their markets and engage in cross-border delivery of goods and services.

Key Threats to the U.S.-Asia & Pacific Trading Relationship in 2022



CCIA identified

150

digital trade barriers in the Asia & Pacific region

92 policies have been enacted

58 are in development

This engagement comes at a critical moment in the relationship. Some countries in the Asia & Pacific region have enacted policies that hinder the ability of U.S. digital services to operate. The following is excerpted from CCIA's annual comments submitted to the Office of the U.S. Trade Representative regarding its National Trade Estimate report—first, there are broad takeaways from the region followed by details of the trends identified in the region.

Digital Trade Barrier Trends for the Asia & Pacific Region in 2022.

Restrictions on Cross-Border Data Flows and Data and Infrastructure Localization Mandates

- **Vietnam**:
  - » Vietnam remains a country of concern for industry as it continues to pursue localization measures. The Law on Cybersecurity took effect January 1, 2019.
  - » The law is expansive and includes both data localization mandates and content regulations. Under the law, covered service providers are required to store personal data of Vietnamese end users, data created by users, and data regarding the relationships of a user within the country for a certain period of time.
  - » On Aug. 15, 2022, the Vietnamese government issued Decree No. 53/2022/ND-CP which added detail to several of the articles under the original Law on Cybersecurity, including potential conflations with the Law including on localization requirements for domestic and foreign companies; a failure to delineate between domestic companies and Vietnamese companies, rendering foreign companies forced to incorporate locally are included; a lack of clarity regarding whether data needs to be kept in Vietnam or whether a copy suffices; and other issues implicating provisions of the Law and other laws regarding data localization, local representation, and data processing.
  - » The Vietnamese government is working on a Personal Data Protection Decree (PDP), but there are concerns of localization requirements based on the current draft, which prescribes conditions that a personal data processor must fully satisfy with regard to the treatment of personal data of Vietnamese citizens, including 'registration' of transfer of such data of Vietnamese citizens overseas, impacting cross-border data flows.

- **Indonesia**:
  - » The Government of Indonesia introduced Government Regulation 71/2019, whereby the storing and processing of data offshore by any "Electronic Systems Providers (ESPs)" will require prior approval from the government. GR 71/2019 provides great visibility on its data localization policy, the implementing regulations continue to be a significant barrier to digital trade and inhibit the ability of U.S. firms to participate in the e-commerce market in Indonesia. The definition of Public Scope ESPs includes public administration, which goes beyond nationals security and intelligence data.
  - » There is also a Ministry of Communications and Informatics Circular Letter which requires all Ministries to obtain clearance from the Ministry for any IT procurement or expenditure to ensure maximum utilization of the National Government Data Center, a challenge for cloud adoption by public agencies and a barrier to U.S. cloud services providers from servicing the Indonesian public sector market.
  - » On September 20, 2022, Indonesia's Parliament ratified its Personal Data Protection bill which differentiates the responsibilities between data controllers and data processors. Data transfer across borders is limited to countries which have equivalent standards of data protection, however there are no guidelines on assessing the level of data protection across countries, which are set to be the subject of further regulations to dictate the implementation of cross-border data transfers. The bill would also impose extraterritoriality as its cross-jurisdictional basis, and applies to any entity located either in Indonesia and/or outside Indonesian but either has legal impact for Indonesia and/or Indonesian citizens located outside of the country.

- **Thailand**:
  - The Personal Data Protection Act went into effect on June 1, 2022, which tracks with some of GDPR, but veers from it in some data transfer regards. The law mostly applies to all entities that collect, use, or otherwise share personal data in Thailand or of residents of the country, with no restrictions regarding their own standing under Thai law or where they themselves are incorporated, or even if they operate in Thailand. The extraterritorial nature of the law reflects an obstacle to U.S. online services providers.
  - The Thai Office of the Personal Data Protection Committee released draft regulations to dictate rules for transferring personal data outside of Thailand under the PDPA, including a provision that could lead to companies needing to obtain consent from customers if they opt to change business partnerships surrounding the sub-processing of data.

- **Pakistan**:
  - In May 2020, the Ministry of Information Technology and Telecommunication (MoITT) released a draft Data Protection Bill that contained provisions on data localization (including an undefined "critical personal data" category), a powerful regulator in a newly established data protection authority, extraterritorial application, and criminal liability.
  - After multiple rounds of public consultation, MoITT released a new version of the bill in August 2021. While some of the provisions around criminal liability and data localization are slightly improved, significant concerns remain regarding impediments to the cross-border flow of "sensitive" and "critical" data. Furthermore, these terms – "sensitive" and "critical" – are ill-defined, with "unregulated e-commerce transactions" falling within the definition of critical data. The draft bill would also introduce and provide broad powers to a new National Commission for Personal Data Protection with the ability to bring forth new regulations and to demand access to data.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

- **India**:
  - There is great concern with the speed at which Indian policymakers and political leaders have increased censorship practices and increased restrictions on companies that fail to take down content political leaders deem "objectionable". Internet shutdowns, the blocking of services, and intimidation of local employees of online platforms have all been features of this campaign.
  - In 2021, amendments to the IT Act went into effect imposing additional requirements under the Intermediary Rules and imposing new obligations on intermediaries, such as strict timelines for takedown requests and significant penalties for noncompliance. Under India's Rules, Intermediaries must remove content within 24 hours upon receipt of a court order or Government notification and deploy tools to proactively identify and remove unlawful content. There are also concerning law enforcement assistance provisions, including a requirement to "enable tracing out of such originators of information on its platform" at the request of government officials.
  - On October 28, 2022, the Ministry of Electronics and Information Technology released the final version of its content moderation amendment, which stipulated that the panel would have the ability to hear complaints from users regarding social media providers' content moderation decisions and reverse such decisions of platforms. The panel is set to be established within three months of the release of the rules, which require social media providers to acknowledge user complaints within 24 hours and address users' requests within 15 days—further, if the request seeks the removal of content, the social media provider would be obligated to address that complaint within 72 hours.

- **Pakistan**:
  - In February 2020, the Ministry of Information Technology and Telecommunication (MoITT) released the Citizens Protection (Against Online Harm) Rules, which after several iterations served as the basis for the "Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021." The law empowers the government to demand online services providers—defined through "any information system"—to take down online content it deems necessary to protect the "glory of Islam", the "security of Pakistan", "public order", "decency and morality", and the "integrity or defense of Pakistan". Online content providers—such as social media companies—would have 48 hours to comply, or the government would have the ability to degrade the providers' services, block the provider, or impose a fine of up to 500 million rupees (about $2.24 million).
  - Additional requirements for online content providers include: mandatory local office presence and registration by the entity providing the service within three months; obligations to appoint a local "compliance officer" to liaise with the PTA on content removal requests; obligations to appoint a local "grievance officer" and post their contact details online (the grievance officer would be required to redress complaints from the public within 7 days of receipt); compliance "with the user data privacy and data localization provisions" of a forthcoming Data Protection Law; intrusive content moderation and monitoring requirements; and providing user data in a decryptable and readable format to investigative authorities in accordance with existing federal law.

- **Indonesia**:
  - The ICT Ministry issued Ministerial Regulation 5/2020 on private electronic systems providers ("ESP"s)—the definition of which includes practically every Internet website or Internet-enabled service—in December 2020, which went into effect immediately. Along with concerning provisions that undermine firms' ability to operate in Indonesia related to registering to avoid the government blocking them in the country, there are broad and extensive online content regulations imposed on online services providers.
  - Under MR 5/2020, ESPs must comply with strict timelines for content removal - 24 hours for "prohibited content removal requests and only 4 hours for "urgent" removal requests. Vague definitions under the new Regulation leave firms vulnerable to fines and/or service restrictions.

- **Vietnam**:
  - The Law on Cybersecurity also includes provisions on content regulation, requiring online services to monitor user-generated content and remove "prohibited" content within 24 hours upon notification from government offices. It also establishes procedures for the service provider to both terminate access for a user posting "prohibited" content and share information regarding the user. "Prohibited" content includes content that is critical or disparaging of the Vietnamese government. Companies have already been fined under this provision.
  - In July 2021, the Vietnamese government proposed amendments to the Ministry of Information and Communication Decree 72/2013, which included all foreign enterprises providing cross-border services with over 100,000 Vietnamese unique visitor access per month having to engage in data and infrastructure localization requirements. Further, digital platforms, including cross-border providers, are required to take down violating content within 24-hours.

- **Bangladesh**:
  - Bangladesh's Information and Communication Technology Act and Digital Security Act both criminalize and restrict online content posted to digital services platforms in restrictive ways. These include criminalizing publication of information online that hampers the nation, tarnishes the image of the state, spreads rumors, or hurts religious sentiment; imposing criminal penalties up to $120,000 and up to 14 years in prison for certain infractions; and prohibiting the transmission of any data or voice call and censor online communications.

- The Bangladesh Telecommunication Regulatory Commission moved to expand its expansive oversight of Internet content through the release of a draft bill called Regulation for Digital, Social Media and OTT Platforms, which was presented in its final form in October 2022. The bill empowers the government to demand online services providers remove content from a user or reveal information about a user if necessary to further the "unity, integrity, defense, security, or sovereignty of Bangladesh," is "offensive, false or threatening and insulting or humiliating" to any person, is harmful to "religious values," is "patently false" or belongs to another person, is seen as oppositional to the "Liberation War of Bangladesh, the spirit of the Liberation War, the Father of the Nation, the national anthem, or the national flag," or a wide range of other vaguely-defined violates, all of which would be determined by the government. Further, the bill would require the outright blocking of information in the case of an "emergency," as defined by the government. The demands for removal or blocking of content could be made with a 72-hour window for compliance, with the threat of blocking the content if a platform does not adhere to the demand.

- **Cambodia**:
  - Cambodia has followed in the footsteps of China's "Great Firewall" that blocks U.S. services providers from entry into the market through the advancement of a sub-decree, signed in February 2021, to establish the National Internet Gateway and create a single point of entry for internet traffic regulated by a government-appointed operator. While the specifics of the implementation remain unclear, this could be abused and misused to block online content.

- **Singapore**:
  - The Protection from Online Falsehoods and Manipulation Bill became effective on October 2, 2019, requiring online services to remove content or carry 'corrections' on their platforms in response to claims from the government or from individuals that content is false or misleading.
  - The Foreign Interference (Countermeasures) Act (FICA) went into effect in July 2022, and requires online services to remove content or carry 'corrections' on their platforms in response to claims from the government or from individuals that content is being covertly influenced by a foreign actor and introduce service restriction guidelines to certain platforms.
  - In October 2022, the Ministry of Communications and Information introduced a Code of Practice for Online Safety for Social Media Services, which would proscribe content moderation practices and "system-wide" safety standards. These procedures would also empower the Infocomm Media Development Authority to compel such companies to block access to harmful—even if not illegal—content for users in Singapore.

Telecommunications-Related Barriers

Countries have sought to leverage regulations historically rooted in telecommunications policy for telephony as a method of restricting digital services providers' access to their markets or to extract revenue from online platforms to bolster local telecommunications incumbents. *Examples include:*

- **South Korea**:
  - Seven proposals have been made by the Korean National Assembly to mandate "network use fee" payments by certain content providers over the past year and a half. This is at times justified by an argument that network fees will help fund the costs of extending and adding capacity to local broadband markets, but is posed to distort incentives and leads to discriminatory treatment of content and application providers. This follows years of conflict among U.S. content providers operating in the region and local telecommunication providers.
  - These proposals have been consolidated into the seventh piece of legislation on this matter, introduced by Rep. Young-chan Yoon, called the "Netflix Free Ride Prevention Act," which would effectively mandate foreign content access providers—namely U.S. firms such as Google, Facebook, and Netflix—to enter into paid contracts with Internet service providers for the content demanded by ISPs' customers.

- **India**:
  - » In September 2022, the Department of Telecommunications released the Draft Indian Telecommunication Bill, which would redefine "telecommunications services" to include a wide range of Internet-enabled services that bear little resemblance to the telephony and broadband services previously governed by this regulatory regime. Telecommunications services providers would then be effectively required to gain a license from the central government.
  - » The provision of licenses would then entail a host of conditions for online services providers including paying into the country's Telecommunication Development Fund, one of the functions of which is to deploy broadband services, along with a host of concerning provisions that could undermine digital security and freedom of expression. The legislation would include a troubling move of authority away from the traditional regulator, TRAI, to a central government authority.

Discriminatory Platform Regulation

In recent years, U.S. technology firms have identified concerns around a rise in protectionism relating to digital competition in the form of targeted regulation and some countries in the Asia & Pacific region pursuing *ex ante* competition approaches that restrict U.S. firms ability to offer services in the region. *Examples include:*

- South Korea:
  - » In August 2021, the Korean National Assembly passed legislation that requires mobile application marketplaces to permit users to make in-application purchases through payment platforms not controlled by the marketplace itself. The scope of the law effectively creates a ban on a predominately used U.S. model, at the exclusion of local equivalents. Further, policymakers supportive of the bill have made clear their intent to single out specific U.S. companies with the new law.
  - » The rules banning app store operators from requiring "specific payment methods" were approved by the Korea Communications Commission on March 8, 2022. U.S. operators of application marketplaces are disincentivized to operate in a region where it is unclear how the application distributor could recover the costs it incurs in maintaining the mobile application marketplace.

- **Japan**:
  - » In May 2021, the Japanese Consumer Affairs Agency (CAA) enacted "Act on the Protection of the Interests of Consumers Using Transaction Digital Platforms". The law aims to impose certain obligations on platforms regarding resolution of disputes between merchants and consumers, and requires platforms to disclose information to consumers about merchants upon request.
  - » On April 26, 2022, the Japan Digital Market Competition Headquarters (DMCH) released interim reports on *Evaluation of Competition in the Mobile Ecosystem* and *New Customer Contacts (Voice Assistants and Wearables)*.
  - » In these interim reports, the DMCH proposed several new avenues for ex ante digital platform regulation in mobile apps and voice assistants and wearables that could disproportionately harm U.S. digital firms without accounting for the broader market dynamics that implicate local and foreign firms, if the regulations fail to incorporate a robust market analysis and pursue heavy-handed ex ante restrictions on certain companies. Problematic proposals and explorations made in the interim reports include forcing digital platforms to share data with third parties and to provide third parties access to data (such as click-and-query search data); restrictions on platforms using data across services; undermining intellectual property by imposing obligatory sharing of trade secrets and copyright; and overly relying on similar actions taken in other jurisdictions that have yet to be genuinely tried and tested.

China's Extensive and Repressive Digital Authoritarianism and Protectionism

The Chinese market continues to be hostile to foreign competitors, and in recent years the focus on U.S. information technologies and Internet services has intensified. An influx of anticompetitive laws directed at information infrastructure, cloud services, data transfers and ecommerce services combined with an uptick in Internet shutdowns have businesses growing more concerned and hesitant to enter the Chinese market, costing American firms.

China remains a very difficult market for Internet services to operate in due to a number of localization and protectionist measures. The United States International Trade Commission has estimated billions of dollars are being lost in the market as a result. The USITC estimates that Facebook loses anywhere from $3.1 billion to $13.3 billion every year, depending on the size its market share were if it could operate in the country. YouTube would lose anywhere from $100 million to $7.5 billion and Google Search could have lost $2.6 billion if it had a small market share and $15.5 billion if it had a large market share in 2021 alone. This is a result of measures including restrictions on the transfer of personal information, extensive requirements on foreign cloud service providers to partner with local firms, and foreign investment restrictions. China also actively censors cross-border internet traffic, blocking some 3000 sites and services, including that of many American online services. These regulations all are fundamentally protectionist and anticompetitive, and contrary to China's WTO commitments and separate commitments to the United States.

Major examples of cross-border services restrictions include the following:

- The 2016 Cybersecurity Law and measures pursued through its mandate such as:
  - » Measures of Security Assessment of the Cross-border Transfer of Personal Information
  - » Measures for Data Security Management
- The 2021 Data Security law
  - » The "Administrative Measures on Data Security in the Industry and Information Technology Sectors," published under the power of the 2021 law
- The Personal Information Protection Law
- China's Standardization Law