2024 Key Threats to Digital Trade

Asia & the Pacific

This document accompanies CCIA's annual National Trade Estimate Report filing. Information and data is current as of October 17, 2024. For the most recent dataset visit digitaltradebarriers.ccianet.org.

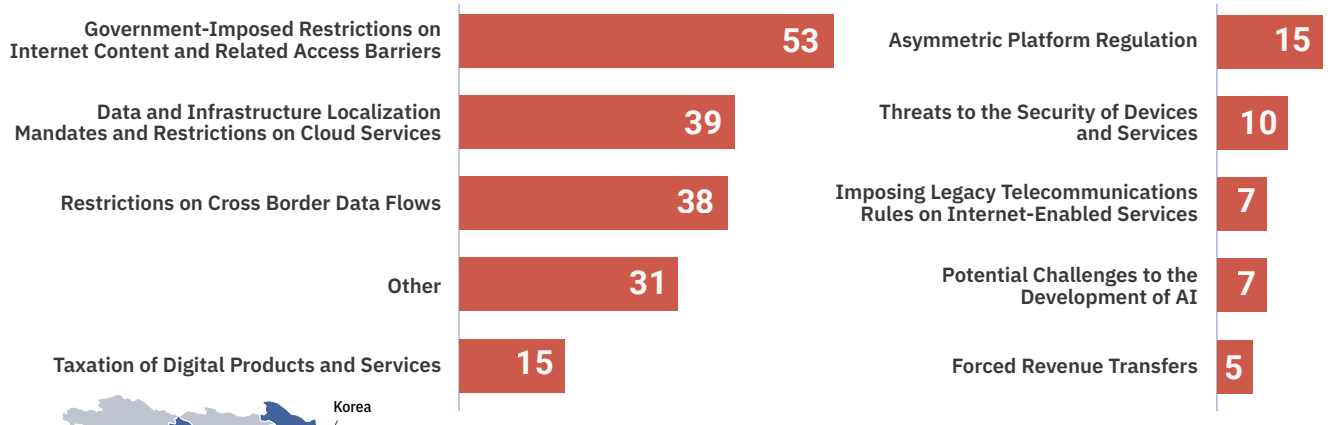
The United States has enjoyed strong diplomatic and economic relationships with the countries in the Asia and Pacific region for decades. Consumers in the United States import billions of dollars of goods and services from firms in the Asia and Pacific region annually as well.

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

Services drive the benefits for U.S. exports in this mutually beneficial relationship, as are digital services. The U.S. generated **$145.1 billion in exports of digitally-enabled services** to the region in 2023, bringing numerous positive externalities for business operations and consumers in the region and a **trade surplus of $50.1 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 2024[1]



CCIA identified

220

digital trade barriers in the Asia & Pacific region

143 policies have been enacted

77 are in development

1 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. https://ccianet.org/library/comments-for-the-2025-ustr-national-trade-estimate-report/

Digital Trade Barrier Trends for the Asia & Pacific Region in 2024

Government-Imposed Restrictions on Internet Content and Related Access Barriers

Australia

- Australia amended its **Criminal Code** in April 2019 to establish new penalties for Internet and hosting services that fail to provide law enforcement authorities with details of "abhorrent violent material" within a reasonable time, or fail to "expeditiously" remove and cease hosting this material. Criticism for the legislation was widespread, with particular concern about the rushed nature of the drafting and legislative process. precluding meaningful stakeholder consultation. The legislation applies to a broad range of technology and internet services, including U.S.-based social media platforms, user-generated content and live streaming services, and hosting services. However, the law does not take into account the varying business models of these services in scope of the law and their varying capabilities or roles in facilitating user-generated content.

- The **Online Safety Act**, passed in July 2021, gives the eSafety Commissioner the power to demand the removal of adult cyber abuse and other content that is deemed "harmful." This legislation also gave the eSafety Commissioner the power to compel eight different sectors of the online industry to develop co-regulatory codes of conduct that detail how companies will prevent both illegal and legal but harmful content from being viewed by minors. While industry responded by developing eight different Codes of Practice (corresponding to the eight different sectors mentioned), the eSafety Commissioner rejected two of those covering relevant electronic services and designated internet services - and instead proceeded, in November 2023, to issue two industry standards for such services. Industry is concerned about strict requirements to invest in systems to detect and remove harmful online content (and the associated need to build Australia-specific policies, products, and systems); the ill-defined concept of "harm" that will lead to lawful content being censored; and disproportionate penalties.

- On December 15, 2022, the eSafety Commissioner released a report detailing responses it received from digital services providers pursuant to the **Basic Online Safety Expectations**, passed through the Online Safety Act. The report detailed platforms' responses regarding efforts to address online child safety and abuse and included condemnation of services that failed to monitor person-to-person video calls for possible child sexual exploitation and abuse (CSEA). The Commissioner announced plans to send additional notices regarding CSEA in early 2023, and to: issue the first periodic notices to begin using one or several metrics to track compliance; publish any extra guidance required; and begin issuing statements detailing compliance and/or non-compliance throughout the rest of the year.

- On July 12, 2024, the Chair of the Competition and Consumer Commission announced a proposed law requiring internet companies to proactively take down scams. The regulation would create a mandatory, enforceable set of requirements for companies to take reasonable steps to protect consumers and offer redress, with potential fines of up to A$50 million, three times the benefit gained by the scam, or 30% of turnover. The obligation would require companies to proactively monitor their services, drastically increasing the costs of operation in the Australian market.

- On September 10, 2024, Prime Minister Anthony Albanese announced the government's intention to impose a minimum age restriction for the use of social media services. To the extent that this legislation implements unreasonable compliance obligations for companies and undermines personal privacy for age verification processes, or requires the adoption of untested local age verification technology, the proposed regulations may warrant U.S. government attention.

Bangladesh

- The **Information and Communication Technology Act** of 2006 (the Act), amended in 2013, authorizes the government of Bangladesh to access any computer system for the purpose of obtaining any information or data, and to intercept information transmitted through any computer resource. Under the Act, Bangladesh may also prohibit the transmission of any data or voice call and censor online communications. The Bangladesh Telecommunication Regulatory Commission (BTRC) ordered mobile operators to limit data transmissions for political reasons on several occasions in 2019 and in 2020 ahead of politically sensitive events, including local and national elections. The BTRC ordered mobile operators to block all services except for voice calls in the Rohingya refugee camps in Cox's Bazar from September 2019 until August 2020.

- The Bangladesh Parliament passed the **Cyber Security Act** in September 2023. The law criminalizes a wide range of online activity, creating challenges for internet-based platforms and digital media firms, retaining almost every single offense detailed in the original law. The Act criminalizes publication of information online that hampers the nation, tarnishes the image of the state or hurts religious sentiment. The law also empowers the government to remove and block content online. The law has come under scrutiny for harming civil liberties and human rights.Upon passage of the bill, the U.S. Embassy in Bangladesh issued a statement noting that the legislation "continues to criminalize freedom of expression, retains non-bailable offenses, and too easily could be misused to arrest, detain, and silence critics."The State Department, in its latest Investment Climate Statements, observed that "the CSA continues to criminalize freedom of expression, and cases have been filed under the new law to harass members of the media, civil society, and opposition groups."

- The Bangladesh Telecommunication Regulatory Commission has proposed a draft of regulations that, if adopted, would grant the government broad-sweeping powers to dictate online content with the threat of extensive punishments for firms and employees deemed non-compliant. The draft of the rules, which have been called the **Regulation for Digital, Social Media and OTT Platforms** and proposed several times over the past year, were presented to a subdivision of the Supreme Court of Bangladesh on January 9, 2023. Despite providing fora for public feedback to the draft legislation, the draft of the bill appears to reflect none of the vast concerns raised by industry and free expression advocates to the Bangladesh government. 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, defence, 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—given that the bill is extraterritorial in nature, these provisions carry additional burdens for foreign services suppliers. Prior iterations of the bill have included criminal liability and possible prison sentences for local employees along with a $35 million fine, and although the most recent draft suggests the effort is moving towards liability for the firm and not individual employees, the lack of definitions in the bill render this a lingering concern.

- Throughout June and August 2024, the Bangladesh Telecommunication Regulatory Commission instructed international internet gateway operators to block access to major social media platforms and messaging services, including Facebook, WhatsApp, TikTok, and YouTube, amidst ongoing social unrest. The Minister for Posts, Telecommunications & Information Technology cited companies' failure to comply with laws on combatting misinformation, without citing specific directives, to justify the blockages — and threatened imposing further regulatory measures, including data localization.

- According to data from Access Now, the internet was shut off three times in Bangladesh throughout 2023 in response to political protests, earning it the distinction of being one of a few countries that has imposed shutdowns in 5 or more consecutive years since 2016. The government imposed further internet shutdowns through July and August 2024, including for an eleven-day consecutive period. In addition to the strong human rights concerns associated with government shutdowns of the internet, there are grave dangers to digital trade as well – as cited by local industry and civil society. As detailed by the U.S. International Trade Commission's two-part investigation into foreign censorship released in February and July 2022, internet shutdowns can cause millions of dollars in losses for U.S. social media and user-generated-video services, representing a notable loss to U.S. services exports.

Cambodia

- Reports of censorship and mandated internet filtering and blocking continue to persist in Cambodia. Legislation passed in April 2020 grants extensive authorities to the government to restrict information online if a state of emergency is imposed. This has prompted concern at the UN over possible human rights abuses.

- A sub-decree signed in February 2021 established the **National Internet Gateway**, which would create a single point of entry for internet traffic regulated by a government-appointed operator. As noted by the State Department's most recent investment analysis from April 2022, "the MOC and MEF issued notification number 837 requiring all companies operating in Cambodia to use a national second-level domain name (.com.kh) as well as an email address with the national second-level domain name when filing annual declarations of commercial enterprises." While the specifics of the implementation remain unclear, there is potential that this could be abused to block online content and keep out certain foreign digital services, akin to China's "Great Firewall, The law was set to go into effect in February 2022 but has yet to be fully implemented. Nonetheless, in February 2023, in the build-up to national elections that July, the Cambodian government swiftly mandated internet service providers to block several domains associated with the Voice of Democracy news outlets.

- Cambodia's Interior Ministry is developing a draft **Cybercrime bill** that could hold intermediaries liable for third party content. The bill also contemplates new data localization mandates. The draft from September 2022 reportedly includes granting the government the power to take control of operating systems and duplicate data from private companies if they are deemed to be unable to address the harms of a cybersecurity threat or data breach. Although not yet finalized, reports indicate that the government is targeting completion of the bill by the end of 2024. The draft, as of April, was not public but reportedly included provisions prohibiting defamation, using "insulting, derogatory or rude language," and sharing "false information" that could harm Cambodia's public order and "traditional culture." These terms are ill-defined and the punishments for violations include fines and imprisonment. The law would also permit the government to gather and record internet traffic data of individuals suspected of committing crimes and would criminalize online material that "depicts any act or activity ... intended to stimulate sexual desire."

Hong Kong

- The **National Security Law** was promulgated in Hong Kong in June 2020. It allows the Hong Kong authorities to request message publishers, platform service providers, hosting service providers and/or network service providers to remove a message deemed to constitute an offense endangering national security; restrict or cease access by any person to the message; or restrict or cease access by any person to the platform or its relevant parts. The Hong Kong authorities have reportedly demanded internet service providers to block access to websites in Hong Kong, and the list of blocked websites under the law, though not officially confirmed by the Hong Kong authorities, appears to be increasing on national security grounds. Hundreds of people have reportedly been arrested under the law, as human rights experts have alerted world leaders to the harms of the law.

- Hong Kong's **Personal Data (Privacy) (Amendment) Ordinance** of 2021 entered into force on October 8, 2021, which included concerning anti-doxing provisions. The provisions empower the Office of the Privacy Commissioner for Personal Data of Hong Kong with the ability to demand that online platforms take down doxing content, the definition of which could include blocks of entire websites or platforms. The application of these demands could extend beyond Hong Kong for content posted anywhere and foreign suppliers are expected to adhere to these demands regardless of where the content was posted. To the extent that these rules lead to the blocking of websites or platforms, the U.S. government should seek to ensure that U.S. business operations in Hong Kong, and the openness of the global internet, are not unduly restricted.

- On March 23, Hong Kong passed the **Safeguarding National Security Ordinance**, which allows the government to punish acts of treason, sabotage, sedition, theft of state secrets, external interference and espionage with heavy jail time, including life sentences. Critics of the law predict that the government's broad new powers under the Bill will significantly chill freedom of expression and speech online. Among other notable clauses, the Bill bans the publishing (defined as communicating "in any form," including speaking and writing) of false or misleading statements while colluding with an external force.

India

- Continued Internet shutdowns have left widespread human rights impacts as well as economic losses. The U.S. International Trade Commission estimated losses of $549.4 million incurred by Facebook, Instagram, YouTube, and Twitter between 2019-2021 due to repeated internet shutdowns. The Indian government conducted 116 internet shutdowns in 2023, up from 84 internet shutdowns in 2022, according to Access Now, the most of any country globally. Between 2016 and 2023, India shut down the internet 771 times, which is more than every other country combined.

- Orders by the Indian government to block websites or take down specific content have long been a feature of the Indian market. However, recent legislative changes relating to digital services will pose greater challenges to U.S. exporters. In 2021, amendments to rules under the **IT Act** went into effect imposing new obligations on intermediaries. The amendments require online intermediaries to prevent the display, upload, modification, publication, transmission, storage, updating and sharing of a broad range of information, including any information that is obscene, harmful to children, deceptive or misleading, and that "threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation". The amended rules also include strict timelines for intermediaries to take down content upon government request and onerous due diligence requirements for certain intermediaries to put in place additional resources and processes for user complaints and redress, monitoring for harmful content, and producing compliance reports. Additionally, the amended rules also include localization requirements, and traceability requirements which could potentially require service providers to break security encryptions, thus posing greater privacy and security risks and having a potentially chilling effect on human rights and future investment along with over-removal and censorship of legitimate content, including political speech. Exacerbating what is a difficult market is India's use of harassment and intimidation tactics through the IT Law to impose restrictions on freedom of expression in the country and coerce preferred behavior from online platforms. As a result, India representing one of the battlefronts of the growing—and concerning—global trend of employee intimidation.

- On July 7, 2023, the Telecom Regulatory Authority of India (TRAI) released a consultation paper dubbed "**Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services**." As part of this consultation, TRAI sought comment on bringing OTT providers into the licensing and registration framework required of telecommunications operators and on the merits of "selective banning" certain OTT services. In addition to the risk of duplicative regulations for OTT

services—including regulations still being developed through the Draft Telecommunications Bill—the proposal raised numerous substantive concerns that would affect U.S. suppliers operating in the market. Key concerns included the unjustified application of telecommunications-style regulations for online services providers despite the fundamental differences between the functions and uses of the services; and destructive harms to freedom of expression and the open internet. In particular, the goal of empowering government entities and regulators to selectively block access to OTT services in India brings serious concerns with respect to internet freedom, privacy, and security. CCIA outlined these concerns in the TRAI proceeding.

- In November 2023, India advised social media companies that they will be held accountable for "deepfakes" posted on their platforms and instructed such companies to remove content from their platforms within 36 hours of receiving a complaint. Failure to do so will result in legal consequences under India's IT rules and could result in the platform losing the protection available under Section 79(1) of the **Information Technology Act**.

- In August 2024, the Ministry of Information and Broadcasting withdrew the latest draft of the **Broadcasting Services (Regulation) Bill**, after initially sharing it with select stakeholders for comment.554 The proposed Bill expanded its scope from traditional broadcasters and platforms with online curated content to also include social media platforms. It would have established regulatory oversight over social media accounts and online video creators and established a broad definition of "digital news broadcaster" to include independent content creators, provoking widespread backlash from stakeholders. While the Ministry announced a deadline for input on the 2023 draft of October 15, some sources indicate that the government will continue to rely on closed-door consultations. The design of this bill and its intent to control social media content in the same way the government does broadcast services raises alarms both for the internet ecosystem and the ability for online services providers to operate in India with regulatory certainty while also raising grave freedom of expression concerns.

Indonesia

- In December 2020 The ICT Ministry (Kominfo) issued **Ministerial Regulation 5/2020** to regulate private electronic systems providers ("ESP"s)—the definition of which includes practically every internet website or internet-enabled service. Under the new framework, local and foreign ESPs are required to register with the government and appoint local representatives to respond to government demands for access to data and information. ESPs are expected to comply with demands for data access for "supervisory and law enforcement purposes'' within 5 days. The process for registering and subsequent punishment for failing to do so is excessively opaque, and enforcement procedures lack transparency. The law stated that ESPs would be given 6 months of transition time to register in Indonesia's database, but Kominfo did not provide guidance until June 14, 2022 for compliance set for July 20. The regulatory uncertainty led to several major U.S., French, and Japanese companies failing to register and being blocked in Indonesia, such as Yahoo, PayPal, Valve, Nintendo, Ubisoft, and others, although several of these companies were eventually unblocked. Pursuant to this regulation, ESPs must comply with strict timelines for content removal, including 24 hours for "prohibited content removal requests and only 4 hours for "urgent" removal requests. Vague definitions under the new Regulation open companies up for large consequences, from fines and/or service restrictions. Civil society groups have also raised concerns with aspects of the Regulation.

- Indonesia's excessive content takedown requests and internet shutdowns have affected U.S. firms financially and implicate broader concerns of freedom of expression online. The USITC estimated $82.2 million in economic losses in Indonesia due to the shutdown of the internet in 2019 affecting Facebook, Instagram, YouTube, and Twitter between 2019-2021.

- The phenomenon of content restrictions continues to expand—between July 2023 and December 2023, Meta reported that the company restricted access to "47 million items allegedly violating local laws on gambling such as the **Electronic Information and Transactions (EIT) Law** and **KOMINFO Regulation 5/2020 on Private Electronic Services Operator**"—compared to 1,458 items removed over the same period in 2022.

- Additionally, the government continues to move forward with the 2019 draft **Bill on Broadcasting** that would place internet streaming platforms under the oversight of the Broadcasting Law, subjecting them to licensing and censorship laws. In March 2024, legislators amended the draft to include greater state control and stricter content standards, sparking alarm from civil society. The law would have implications both for the delivery of online services and the open internet as well as freedom of expression online.

- After a decade-long revision process, the Parliament passed a new **Criminal Code** on December 6, 2022, which increases liability for digital platforms, including provisions relating to religious blasphemy, insulting the President and the Vice President, and expressing views counter to the national ideology (Pancasila). Corporations are now subject to criminal law under the code. The draft includes provisions subjecting corporations to criminal law, meaning business decisions, administrative issues, and negligent behavior could be penalized criminally (Article 45- Article 50). There is much ambiguity and uncertainty about the interpretation of the clauses and how they will be enforced (i.e., if all Indonesian laws applicable to individuals will then be applied to corporations). Detailed provisions will be stipulated in the implementing regulations. The new provisions could potentially impact how platforms moderate content for topics such as misinformation and slander (such as insults to the President and Vice President).

- In 2024, under the **ICT Ministry's Decree 172**, the Ministry is mandated to operate a 'content moderation compliance system' ('Sistem Kepatuhan Moderasi Konten') to implement content takedown notices and issue corresponding fines. The Ministry stated publicly that the system - carried out via a platform called SAMAN - is live and enforced as of September 2024. Industry remains concerned about the lack of clear directives from the Ministry on the platform's operational readiness – including a lack of information about the appeal mechanism, turn-around-time and fair fine calculation, questionable security, and absence of an industry accepted technical guidelines.

Nepal

- On Aug. 8, 2023, Nepal's Cabinet passed the **National Cyber Security Policy**, which adopted a "National Internet Gateway" similar to that passed and pursued by Cambodia in 2021. This measure seeks to implement a government-owned intranet and an internet filtering system—a national internet gateway—that would restrict what content is visible online in the country. The policy would implement a regime of monitoring what is posted online in the country and restricting what can be seen by internet users. This represents a threat to the internet ecosystem and to the availability of U.S. services in the country, would limit competition and increase operational barriers, and is viewed by industry as an effort to exert tighter control over the internet, ensuring centralized monitoring over all traffic. The broad impact on human rights is described by Digital Rights Nepal and International Center for Not-for-Profit Law detail in a joint brief: "Implementation of the [National Internet Gateway] presents a profound risk of censorship and threatens the fundamental right to freedom of expression. By consolidating all internet traffic through a centralized point, the government gains unprecedented control over the flow of information, enabling them to regulate and censor online content according to their own agenda." As the civil society group Article 19 elaborates, the concern is that "if Nepal's national internet gateway is modeled on others in the region it would mean centralising control of all internet traffic in and out of the country through a government-appointed operator, potentially supercharging surveillance and censorship capabilities while leaving open very serious questions about data privacy and protection, and the risk of criminal penalties for telecommunication companies."

- In November 2023, Nepal's cabinet adopted the '**Social Media Directive**' in an effort to address sectarian violence in the country. The Directive imposes local registration mandates as well as onerous content moderation requirements that lack safe harbor provisions. The Nepal government is subsequently developing a 'Social Media Usage' Bill, which would put in place even stronger requirements for online services providers in place of the Directive.

Pakistan

- The "**Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021**" was published and enacted by the Ministry of Information Technology and Telecommunication (MoITT) on October 13, 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 defence of Pakistan." Online content providers—such as social media companies—would have 48 hours to comply, failing which the government would have the ability to degrade the providers' services, block the provider, or impose a fine of up to R500 million (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. Local and foreign companies have raised concerns over provisions that would pose significant obstacles to participating in Pakistan's market, including requirements to use mechanisms to monitor and block livestreaming content, take down content within short timeframes when the authorities issue demands, and disclose data to authorities in decrypted and readable formats. These rules greatly jeopardize the ability of U.S. firms to operate in Pakistan and undermine freedom of expression in what is a sizable market.

- The government has repeatedly deployed internet shutdowns in response to protests and elections, imposing large economic losses and harming human rights. Industry has reported that shutdowns have introduced significant uncertainty and encouraged investment flight. In February 2024, a ten hour shutdown of the internet by the government led to an estimated $18.5 million in lost income. In August 2024, local industry began reporting on the government's implementation of an internet firewall to moderate content – triggering widespread network disruptions. According to local industry groups, the firewall has already cost the economy $300 million, with further costs and harms to human rights expected to increase.

Singapore

- The Protection from **Online Falsehoods and Manipulation Bill (POFMA)** came into effect on October 2, 2019. The law 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 false or misleading. The process whereby the government flags content as false or misleading is opaque and lacks an adequate oversight process. Instead of enhancing trust online, these rules could spread more misinformation while restricting platforms' ability to continue to address misinformation issues. Stakeholders have raised concerns with enforcement of these laws since they went into effect, with early use cases of the law that involved demands to take down political speech and media platforms ahead of the July 2020 general elections. After Singaporean citizens, US social media companies have been the largest target of cases under POFMA, and several have since ceased allowing political ads as a result.

- In October 2022, the Ministry of Communications and Information introduced amendments to the **Broadcasting Act**, including 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 (IMDA) to compel such companies to block access to harmful—even if not illegal—content for users in Singapore. The guidelines were finalized on July 17, 2023, and went into effect on July 18, 2023, with Facebook, HardwareZone, Instagram, TikTok, Twitter, and YouTube the initial companies named as subject to the Code. The guidelines released by IMDA for companies' adherence to the Code include vague directions to address specified content including "content that is likely to cause harassment, alarm, or distress;" "content relating to vice, unlawful gambling, illegal moneylending, trafficking in persons, cheating, fraud, and extortion;" and "content relating to the incitement of violence, mass disorder, or rioting, whether in general or targeted at persons based on their characteristics." While many of these directions could apply to objectionable content that most online services suppliers would normally prohibit or restrict from their platforms, the directions could also apply to reasonable content such as satire, art, or protests, depending on the situation.

- On November 9, 2022, the Parliament passed legislation imposing new obligations on social media providers in the **Online Safety (Miscellaneous Amendments) Bill**. The bill took effect in February 2023. The bill requires large "online communications services" ("OCS"), which include social media services, to comply with a Codes of Practice, and empowers the IMDA to regulate specified categories of "egregious content" that can be accessed through an OCS. The law makes providers of "electronic services"—defined as online services that connect to Singapore and are not explicitly communications or internet service providers—liable for content posted on their platforms. The legislation requires services to remove "egregious content" from its platforms, which includes content that "advocates or instructs on suicide or self-harm;" "advocates or instructs on violence or cruelty" against other people; "advocates or instructs on sexual violence;" shows nudity of a child; restricts or harms public health measures; stokes racial or ethnic hatred; and promotes or instructs terrorism. The IMDA will be empowered to issue demands to remove content or restrict service to specific users, and if companies fail to comply, the IMDA can block the service provider in question.

- A separate bill, the **Online Criminal Harms Bill ("OCH Bill")**, passed on July 5, 2023. The law gives the government more powers to issue "Government Directions" when there is reasonable suspicion that online activity is being carried out to commit a crime specified in the First Schedule of the OCH Bill, or when it is suspected that any website, account or online activity is being used for scams or malicious cyber activities. These include: offenses relating to terrorism and internal security, harmony between different races, religion or classes, trafficking of controlled drugs and psychoactive substances, unlawful gambling, illegal moneylending, and sexual offenses (e.g. distribution of child sexual abuse material or voyeuristic and intimate images without consent). The Online Criminal Harms Act (OCHA) partially took effect in part on February 1 2024, including "directions to online services to restrict the exposure of Singapore users to criminal activities on their platforms," "orders to limit further exposure to the criminal activities being conducted on platforms of non-compliant online services," and "powers to require information to administer the Act and facilitate investigations and criminal proceedings."

Sri Lanka

- Sri Lanka certified their **Online Safety Act** on 2024 which regulates content by prohibiting online communication of false statements and punishing violators with up to five years in prison and/or a fine not exceeding five hundred thousand rupees. The Act also establishes an Online Safety Commission and allows the Commission to order internet service providers and internet intermediaries to remove online posts declared "prohibited statements." Human rights organizations like Amnesty International have criticized the bill, calling it a "major blow to human rights" and a weapon that could be "used to undermine freedom of expression and suppress dissent."

Thailand

- CCIA has previously raised concerns with the **Computer Crime Act**, amended in 2016. In November 2019, the Ministry of Digital Economy and Society established an Anti-Fake News Center to combat what is considered "false and misleading" in violation of the Computer Crimes Act, which has been leveraged to expand oversight of content and identify millions of posts. The regulation adopted a broad definition of "National Security" to cover a wide range of content for which the government seeks the power to demand takedowns.

- In 2019, Thailand passed a controversial **Cybersecurity Law** following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance. Under the new law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency."

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 the government. It also establishes procedures for service providers to both terminate access for a user posting "prohibited" content and share information regarding the user (information service suppliers may not have, if data is encrypted). "Prohibited" content is vaguely defined as any content that is critical or disparaging of the Vietnamese government. Companies have already been fined under this provision.

- Besides regulatory roadblocks, U.S. companies face challenges from technical interventions, at the behest of the government, such as throttling or limiting server access. These technical interventions are part of the government's effort to influence and control content, and undermine U.S. companies' competitiveness in the marketplace.

- On October 1, 2022, the Authority of Broadcasting and Electronic Information issued **Decree 71/2022/ND-CP (Decree 71)**, amending Decree No. 06/2016/ND-CP on the Management, Provision, and Use of Radio and Television Services by extending broadcast television regulations to video on-demand services. Decree 71 continues long-running effort to regulate internet-enabled subscription video services provided on a cross-border basis, and requires such services to be made only through websites or applications with domain names and IP addresses managed by Vietnam. It remains unclear whether wholly owned foreign firms can supply such services, and many popular foreign services have entered into partnerships with Vietnamese ISPs. This decree also limits foreign-controlled advertising on such services.

- On July 17, 2023, the Vietnamese government released a proposed draft decree to replace Decree 72/2013 regulating the management, provision, and use of Internet services and online information. Per the proposed rules, all foreign enterprises providing cross-border services with over 100,000 Vietnamese unique visitors per month must collect and store a wide range of data on Vietnamese users. This data could then be demanded by local authorities upon written request. Cross-border services suppliers are also obligated to monitor and remove information and services deemed illegal and to respond to takedown demands of the MIC and work to prevent such content. However, the rules do not provide clear guidance for how companies can achieve these goals or scan for content at issue. The content-related obligations to prevent violations of domestic laws and policies online are onerous and sweeping, especially in light of the broad definitions of what prohibited acts could entail. In addition, digital platforms, including cross-border providers, are required to take down illegal content within 24-hours once notified by the MIC and to temporarily block content following user complaints within 48 hours. The draft Decree includes concerning and poorly-defined obligations for online platforms to enter into "cooperation agreements" with Vietnamese press agencies where their content is cited. Further, the draft Decree requires all apps offered on app stores to be licensed, while also mandating that online,

multi-player, and interactive game providers must secure licenses for publication of the game in Vietnam. The processes associated with this licensing process are onerous, particularly for foreign companies, as it effectively mandates foreign suppliers to work through local publishers.

- Although the latest draft has not been published, MIC clarified one addition, the adding of user's mobile number as a verification requirement. for online services. This will provide another layer of user surveillance without clear safeguards. At the same time, it also creates a new barrier to trade as it increases the cost burden for cross-border service providers (i.e. the need to engage local mobile phone operators to verify users in the country). In addition, the draft added requirements for collection and storage of personal data (including Vietnam mobile numbers), which is beyond what foreign companies operating in Vietnam need to operate their business, and unnecessarily increases business cost and operational burden. Foreign companies do, in some cases, use mobile numbers for authentication, but typically do not store this data---a requirement also goes against the personal data minimization principle. The use of national citizens' identity (ID) numbers and requirement for verification of ID pose similar challenges for foreign companies as they are not in position to identify whether an ID is fake or not.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Australia

- In 2019, the Australian Government released the **Hosting Strategy**, providing policy direction on how government data and digital infrastructure implements the Digital Transformation Strategy, focusing on certification of data center facilities, infrastructure, data storage and data transmission. In March 2021, the certification framework for the policy was released. Certification requires hosting providers, data center operators, and cloud service providers to allow the government to specify ownership and control conditions. The framework has the effect of imposing data localization, data residency, and personnel requirements on all protected-level data and data from whole-of-government systems.

India

- In 2020, the Ministry of Commerce and Industry's Department of Promotion of Industry and Internal Trade (DPIIT) extended local content requirements to the public procurement of software and services. Based on this Notification, the local content requirements necessary to qualify as a "Class I" supplier is 50% and for a "Class II" Supplier, 20%. The formula for calculation of Local Content has yet to be defined and has been left to the discretion of the different procurement agencies. This policy significantly impacts multi-national companies that rely on global R&D and therefore cannot assign the cost of development to one country (e.g., India); in addition, investments made in the ecosystem (such as construction of data centers or investments in startups) have been discounted. DPIIT's order imposed a significant compliance burden for U.S. and other foreign software and cloud service providers to by requiring that they demonstrate their contribution to the local market as a condition of participation. This framework fails to consider how foreign cloud services providers contribute to India's technology sector and boost local providers' competitiveness by upskilling the workforce and investing in areas such as cloud innovation centers and quantum computing laboratories. Even if cloud services providers are not bidding directly for government contracts, their customers are required to verify their percentage of local content. In cases where cloud services are a significant proportion of cost in a public procurement bid, the percentage of local value add from a cloud services provider becomes crucial. The Indian government is currently planning to further and raise the minimum local content requirement for Class I suppliers to 60% and Class II suppliers to 30%.

- In February 2021, guidelines regarding geospatial data and associated services were introduced with the goal of deregulation and liberalizing India's mapping policy. However, some aspects of the new guidelines are discriminatory towards foreign service providers. Specifically, Indian companies are given

preferential access to geospatial data through prohibitions on foreign entities from creating and owning geospatial data above a certain threshold. While foreign entities can obtain a license for such maps or data through an Indian entity provided it is used only for the purpose of serving Indian users, subsequent reuse and resale of such maps and data is prohibited. There is also a data localization requirement for such data, which has to be stored and processed on a domestic cloud or on servers physically located in India. Compliance with the guidelines is mandatory.

- In April 2022, India began to tighten its restrictions on cloud services providers and virtual private network (VPN) providers through highly intrusive requirements promulgated by India's Computer Emergency Response Team (CERT). Based on these requirements, cloud service and VPN providers must collect personal information—including customers' names and IP addresses. VPN, cloud, and several other IT services providers would be required to log their customers' activity and surrender that information to Indian authorities when demanded. Firms that decline to undergo this broad-sweeping surveillance on their users would have to leave India's prominent market. As a result, many VPN operators left the market due to the regulatory uncertainty and impending invasive oversight, undermining digital security and services exports to the country.

- Industry reports concern that Indian Telecom licensees are obligate to connect their networks only with telecom equipment that has been tested and certified under the Mandatory Testing and Certification Framework (MTCTE). The mandatory testing and certification scheme is in place for certain IT and telecom products, with the justification being a need for safety, functionality, and security. The scope of this requirement was recently increased to include cloud software (such as hypervisors). This hinders the ability of U.S. exporters to access the Indian market absent high compliance costs and a reworking of companies' testing and manufacturing procedures.

Indonesia

- The Minister of Fisheries and Marine Affairs issued **Decree 14/2021** mandating that all subsea cables in Indonesian waters follow 14 prescribed routes and utilize landing points in Manado, Kupang, Papua, and Batam. More than half of existing cables are located out of these prescribed corridors, and following such prescribed routes and landing points lack sound justification. Further, different ministries interpret the landing points differently, and industry reports a lack of clarity over the process to propose new corridors. This restricts the ability of U.S. cloud and infrastructure services providers to determine the best business case for such landings and gives preferential treatment to domestic providers, creates significant business uncertainty, and serves as a hindrance to U.S. economic interests.

- Further, as part of the new **GR 5/2021** rules on business licensing, subsea cable permits require a series of licenses from several Ministries such as Environment, ICT, Transport, and Investment. Requirement from the ICT Ministry include requiring foreign operators to partner with a local network operator that has been operational for five years and completed 100% of construction commitments for the first five years; including the local partner in the cable consortium; meeting minimum of 5% stake by the local partner; and an obligation to land the cable in Indonesia (i.e., precluding transiting Indonesian waters). Such requirements are significant market barriers for U.S. providers to establish their business operations in Indonesia.

- Indonesia significantly restricts the use of public cloud technology in the services industry. Financial service regulators have the authority to further regulate financial sector data in compliance with the aforementioned GR 71. The amended regulations issued by the Indonesian financial regulator, the Otoritas Jasa Keuangan ("OJK"), allow some financial data to be transferred and stored outside of Indonesia with approvals from the respective regulator. While the Bank of Indonesia has adopted a risk-based approach in its payment regulations, it still considers cloud services as a high-risk activity, which requires financial institutions to seek its approval before moving workloads to the public cloud

(**Regulation No. 22/23/PBI/2020**). Meanwhile, with **Regulation No. 11/POJK.03/2022**, the OJK only requires banks to submit approvals if the data center is located offshore. There is no need to submit approvals for cloud use in-country, thus explicitly discriminating against cross-border data processing. Indonesian financial services are still blocked from using offshore data centers. The Bank of Indonesia still requires many categories of financial payments (e.g., debit card transactions) to be processed domestically. OJK has incrementally allowed some electronic systems to be processed offshore in the banking and insurance sector, but this has not been permitted in sectors including multi-financing and lending-based technology. Industry reports these rules are motivated in part by regulators' lack of trust in multilateral law enforcement systems. Industry reports that to operate in Indonesia, compliance with the policy continues to be burdensome and highly restrictive. Further, the OJK requires financial institutions to seek its approval 2 to 3 months before moving workloads to the public cloud. For instance, **Regulation No. 38/POJK.03/2016** requires commercial banks planning to operate an electronic system outside Indonesia to seek approval from the OJK 3 months before the arrangement starts. In addition, financial institutions that plan to outsource the operation of their data centers or disaster recovery centers must notify the OJK at least 2 months before the arrangement starts. Lastly, **Regulation No. 9/POJK.03/2016** only allows commercial banks to outsource "support work" (i.e., activities that are low risk, do not require high banking competency and skills qualification, and do not directly relate to operational decision-making). These workloads that can be outsourced are all subject to the same regulatory requirements, with no differentiation in terms of materiality, unlike in other jurisdictions, such as Australia and Singapore.

Malaysia

- In November 2020, the new Minister of Transport abruptly revoked a 2019 exemption to the **Merchant Shipping Ordinance 1952** that permits non-Malaysian ships to conduct submarine cable repairs in Malaysian waters. The exemption is key in reducing the time required to conduct submarine cable repairs. The cabotage policy adds complexity, time, and cost for submarine cable owners that need to conduct repairs for cables that land in Malaysia. Due to the high costs of vessels for submarine cable repairs and the scarce availability of ships, submarine cable owners require regional and global economies of scale to recoup the large annual investments that are directly undermined by restrictive cabotage policies such as Malaysia's that obstruct repairs. Submarine cables are the global backbone of the internet, carrying around 99% of the world's internet, voice and data traffic, including the backhaul of mobile network traffic and data for digital trade. The revocation was a means to protect the domestic shipping industry from foreign competition. In May 2022, Malaysia's transport minister Wee Ka Siong said the revocation would remain, and that the requirement for foreign vessels to obtain a Domestic Shipping License is "not a hindrance" to submarine cable projects. While the government reinstated the cabotage exception on June 2, 2024, the situation remains uncertain given the billions of dollars of investment in crucial telecommunications infrastructure being dependent on an exemption that can so easily be rescinded once more upon another government change. Industry would benefit from a permanent revocation of the cabotage policy, or a permanent exemption.

- The Malaysian Communications and Multimedia Commission (MCMC) crafted rules that subject data centers and cloud service providers to licensing obligations under the **Communications and Multimedia Act 1998 (CMA 1998)**. Traditionally, and pursuant to global best practices, these licensing requirements are tailored to telecommunications and services providers, rather than a broader class of technology services. Under the new obligations, cloud service providers are required to comply with the provisions of the Communications and Multimedia Act 1998, including requirements on 1) data access and disclosure requests; 2) the interception of communications subject to the discretion of the Communications and Multimedia Minister; 3) mandatory standards periodically set by MCMC; and 4) make mandatory payments to the Universal Service Provision Fund. These new rules went into effect on January 1, 2024.

Nepal

- In March 2024, the Ministry of Communication and Information Technology introduced the draft **Information Technology and Cyber Security Bill 2080** to regulate activities related to information technology and cyber security. As written, the Bill would require data centers and cloud service providers to obtain licenses subject to yearly renewal and would require health and financial organizations to store all data domestically.

Pakistan

- Pakistan established a **Cloud First Policy** in 2022 that implements data localization requirements on broad categories of data identified as "restricted," "sensitive," and "secret." Further, the State Bank of Pakistan prohibits financial institutions from storing and processing fundamental data troves on offshore cloud services. These data localization requirements are ineffective at enhancing data protection while simultaneously making the costs of compliance excessive for U.S. suppliers, which represent a potential barrier to participation in the market.

The Philippines

- The public procurement preferences for domestic entities extend to the cloud sector, restricting foreign and U.S. suppliers' activities in the Philippines market absent domestic partnership. Industry continues to offer cloud services in the Philippines but is concerned that foreign providers are subjected to a mandated licensing process administered by the Securities and Exchange Commission (SEC) in the country as a condition for providing cloud services to the public sector. Absent an SEC license, entities seeking public sector procurement are forced to work with domestic entities, reflecting a de facto obligation.

- Industry reports that the Philippines government has been considering a draft Executive Order dubbed "**Policy Guidelines on Data Localization of Data Stored in the Cloud**" with concerning data localization provisions. The original draft of the EO, first released in 2023, required all data, including non-sensitive and commercial data, that is in any way connected to government work be processed and stored in the Philippines. Further, the EO explicitly stated that the following entities would be mandated to process data using local infrastructure: "Core operations of Bangko Sentral Supervised Financial Institutions deployed on private cloud;" "Health information systems of health service providers and insurers;" "Subscriber information of service providers located in the Philippines;" "All National Security Systems;" and "All sensitive personal information processed by private entities which are also classified as confidential under existing laws." Although the status of the draft EO has not been communicated to industry, it warrants close monitoring by the U.S. government, as the original version appeared to apply so broadly that commercial services would be highly likely to be subject to the data localization mandates. Given the results of such an outcome, which will severely restrict the ability for online services providers—and non-digital services providers such as financial services—to operate in the Philippines, industry remains concerned about this EO.

Singapore

- On May 7, the Parliament passed an amendment 811 to the **2018 Cybersecurity Bill** to broaden the number of entities subject to reporting obligations and increase potential penalties for non-compliance. The amendment expands covered entities to include Foundational Digital Infrastructure providers, such as cloud computing providers and data center facility services, even when located wholly overseas.

South Korea

- On August 19, 2024, Korea's cabinet approved amendments to Korea's 2018 **Electronic Commerce Act (E-Commerce Act)**. The proposed amendments are now under consideration by the National Assembly. Although motivated by a legitimate interest in addressing consumer complaints relating to imported physical goods, particularly from China, this approach is problematic: a requirement for local a agents present in Korea to resolve disputes and the mandatory assignment of such functions to any subsidiary a foreign firm happens to have in Korea is likely inconsistent with Korea's trade commitments under KORUS. Designating a local agent for information exchange would be consistent with FTA local presence rules (e.g., Article 12.5 of KORUS). However, requiring the agent to fully resolve such disputes and assigning such functions to any existing local subsidiary would be tantamount to requiring establishment, and hiring related personnel, that the trade rules are designed to prevent, in cases a supplier prefers to offer a specific service fully on a cross-border basis. The burden this proposal would place on firms offering digital products and services (apps, videos, cloud computing), as opposed to physical products, is noteworthy: such suppliers typically operate global platforms staffed from various locations specializing in specific functions such as payments, technical support, dispute resolution, etc. While most large U.S. digital firms maintain a local presence in Korea, the personnel there may have no expertise or responsibility for complaint dispute resolution, and saddling such an entity with such functions is neither appropriate nor effective.

- The Korean government continues to maintain a highly-effective protectionist stance to keep global cloud service providers out of the local public sector market. It has accomplished this through the Korea Internet & Security Agency (KISA) **Cloud Security Assurance Program (CSAP)**, a set of requirements designed to ensure that public institutions relying on commercially-supplied cloud computing services benefit from secure and reliable cloud offerings. Three main technical requirements have prevented all global CSPs from being able to obtain the CSAP: physical separation of government data, requiring dedicated data centers; non-recognition of Common Criteria (CC) certification of equipment, in favor of unique national requirements; and use of domestic encryption algorithms. In addition, requirements to store and process data domestically and rely exclusively on Korean nationals for the management of services severely affects foreign suppliers' ability to compete in the market. The CSAP obligations have resulted in U.S. firms being effectively unable to qualify to bid on the vast majority of public sector cloud computing contracts, despite WTO and KORUS FTA commitments that provide U.S. firms with that right, and which prohibit the use of technical requirements as a means of denying market access.

- On January 31, 2023, Korea's Ministry of Science and ICT (MSIT) promulgated a revised version of the CSAP. Despite introducing some minor flexibility with respect to data deemed low-tier (i.e., with respect to physical separation), U.S. services remain stymied at every level of CSAP certification—Low, Moderate, and High—with the result that public sector contracts go exclusively to Korean national firms. While burdensome requirements even at the low tier remain (e.g., with respect to encryption), a small portion of the public sector market could be opened to global CSPs, by allowing logical versus physical separation of data for this category. To date, however, no foreign company appears to have obtained such certification. The key burden of requiring physically septate computing facilities for medium and high-tier systems remains. Recent advancements in AI technology, a specialty of U.S. suppliers, are expected to offer significant benefits to the Moderate tier of the public sector. Depriving the Korean public sector access to the most advanced global AI services may be an inevitable result of this restrictive policy. Given Korea's interest in developing its AI capability, allowing for logical separation in the Moderate tier, and alignment with international standards, should be a priority.

- In early 2024, MSIT proposed revisions of the **Notice on Security Certification of Cloud Computing Services**, amending the requirements governing the CSAP. Apart from minor improvements with respect to low-tier data, the revisions ultimately failed to address any other key barriers preventing the Korean public sector from accessing services offered by trustworthy foreign suppliers. The key restrictions

proposed to remain for mid- and high-tier data include requirements to: physically separate facilities used for servicing the public sector from those servicing commercial customers (which was allowed for low-tier data); exclusively use equipment, resources, and personnel located in Korea; exclusively store data in Korea; exclusively utilize Korea's national encryption algorithms; and exclusively rely on NIS certification for key infrastructure.

- The government also requires CSAP-like controls in other sectors, such as in healthcare, with the Ministry of Health and Welfare (MOHW)'s recent inclusion of CSAP-like controls—such as the physical location of cloud facilities, data residency, and CC certification obligations—as a requirement for Electronic Medical Record (EMR) system providers who seek to use public cloud services. While MOHW claims that the CSAP is not mandatory, it plans to provide medical insurance reimbursement premiums only to medical institutions with certified EMR systems, thus creating an unlevel playing field for companies who are unable to satisfy the CSAP-like controls. Similar restrictions have been considered for the education sector.

Taiwan

- In August 2023, the Financial Supervisory Commission (FSC) published amendments to the **Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation**, which stipulate the rules for financial institutions to obtain FSC's permission prior to using cloud computing services. The new amendments seek to simplify the application process, which requires submitting up to 17 documents, responding to duplicate audit requests, and a lengthy review process. Industry remains wary that failure to simplify the process could discourage financial institutions from using cloud computing services, all of which limits market access for U.S. cloud services providers.

- In addition to the Cloud Outsourcing Regulation for financial institutions, the FSC also issued a regulation for insurance firms in December 2019. However, there are still no cloud outsourcing regulations for securities, futures, and investment trust and investment advisory enterprises. Industry reports a lack of clarity for cloud outsourcing regulations that has hindered U.S. cloud service providers' ability to contract with firms in these sectors, who themselves state regulatory uncertainty restricts them from adopting cloud services.

- While Taiwan's sectoral regulations, such as financial services, health records and public sector, allow institutions to outsource workloads to overseas cloud service suppliers, regulators clearly indicate a preference for data localization, stating that "in principle, where customer data is outsourced to a cloud service provider, the location for processing and storage shall be within the territories of the R.O.C.," and, in the case of overseas outsourcing, "except with the approval of the competent authority, backups of customer important data shall be retained in the R.O.C." If an institution seeks approval for overseas outsourcing, it must bear over-burdensome documentary requirements that may cause unnecessary compliance costs; even if an institution is willing to bear the burden, the review process is lengthy and unpredictable; and, the institution still need to maintain a local copy of "important" data.

- Regulations have been promulgated in both the financial services and health industries advancing data localization requirements. For financial services, industry reports that regulations require that material financial customer data are stored in Taiwan, unless the regulatory agency grants an exemption. In the healthcare sector, regulations governing **Electronic Medical Records Management** mandate that medical data remain stored in Taiwan absent an exemption. For both types of data, industry is left with vague and unclear regulations delineating the process for obtaining an exemption.

- Through a September 2023 draft amendment to the **Cybersecurity Management Act (CSMA)**, sectoral regulators would be directed to adopt rules delineating the criteria and the procedure behind the labelling of a critical infrastructure (CI) provider. The draft defines CI as "physical or virtual systems or networks, used in the critical fields formally announced by the Cabinet, once discontinued from operation

or becoming less effective, would lead to significant negative impact upon the national security, public interests, living standard of citizen and economic activities." The draft does not detail how the Cabinet should select and choose the so-called "critical fields," which foments uncertainty.

Vietnam

- On June 3, 2020, Vietnam's Prime Minister signed **Decision 749/QD-TTg**, announcing the country's National Digital Transformation Strategy by 2025. The Decree calls for the creation of technical and non-technical measures to control cross-border digital platforms.

- The Ministry of Information and Communications (MIC) has subsequently issued **Decisions 1145** and **783** which include a local cloud standard and cloud framework, respectively, and set forward technical standards and considerations for state agencies and smart cities projects that offer preferential treatment to local private cloud providers. Such preferential treatment is inconsistent with Vietnam's government procurement obligations under CPTPP. The MIC Minister has stated a desire for Vietnamese firms to attain a stronger hold in cloud computing and digitalization infrastructure, comparable to what they have with facilities-based telecommunications networks. While the standards are technically voluntary, in practice, they are expected to be adopted by the Vietnamese public sector.

- **Decree 53** on the **Law on Cybersecurity** expands data retention requirements for domestic and foreign enterprises. Industry reports that the Law's provisions hinder the ability of cloud service providers to operate and prevent full market access to the technology and security choices that are typically afforded to firms through a competitive cloud marketplace.

- Vietnam allows for foreign participation in the telecommunications sector, with varying equity limitations depending on the specific industry. The **Law on Telecommunications (Telecom Law) 41/2009/QH12** stipulates that domestic companies providing basic telecommunication services with infrastructure can only have 49% foreign ownership, while companies that supply telecommunications services without infrastructure can go up to 65% foreign ownership. Vietnam's regime permits up to 70% foreign ownership for virtual private network (VPN) services suppliers. Facilities-based operators are mandated to be state-controlled firms, which in practice means that the state (through the relevant line ministry) would be required to have at least 51% of equity. For TPP countries, Vietnam committed to offer more lenient treatment, but implementation of this promised liberalization is unclear.

- The revised **Telecom Law** went into effect in July 2024, and adopted a more liberalized regime for OTT services, data centers, and cloud services. The Ministry of Information and Telecommunications (MIC) has drafted a Decree implementing the Telecom Law and has sought industry's feedback. The final draft is under final review by the Government Office, but the extent to which foreign participation is streamlined in the market warrants close monitoring from the U.S. government in a key market, particularly as companies relocate to Vietnam from China.

Restrictions on Cross-Border Data Flows

Bangladesh

- In November 2023, the Cabinet of Bangladesh gave initial approval for a draft personal data protection bill dubbed the **Personal Data Protection Act, 2023**. The legislation contains potential barriers to cross-border data flows. While efforts were made to restrict data localization measures to "classified data" only, in response to earlier industry concerns, the law nonetheless allows the government to determine what data is considered "classified." This would allow the government to regulate international data transfers as they see fit, leaving the contours of the data transfer regime vague and uncertain and hindering the uptake and delivery of online services by U.S. and other foreign providers.

India

- After years of development and numerous iterations, the **Digital Personal Data Protection Bill** was passed and entered into law on August 11, 2023. The bill gives the Indian government broad discretion in interpreting terms in the law such as "potential impact on the sovereignty and integrity of India;" "risk to electoral democracy;" "security of the State;" and "public order." The law institutes affirmative consent for all data processing and includes excessively narrow definitions for activities that could be deemed as legitimate bases for data processing. The law also allows the Central Government to deny the export of data to a country if it so chooses and is able to create a list of jurisdictions where personal data cannot be exported to from India, with no avenue for recourse, such as standard contractual clauses, and no clarity on the criteria for jurisdictions to be on the list. Coupled with the law allowing for the data localization requirements to be prescribed under other legislation (e.g., those governing the financial services sector), this results in significant uncertainty for industry in the overall environment for data protection and cross-border data flows.

Indonesia

- In 2019, the government of Indonesia issued **Government Regulation 71/2019 (GR 71)** to revise the previous **Government Regulation 82/2012 (GR82)**. While this measure improved many aspects of data governance, certain data localization mandates were retained – while GR 71 relaxed data localization requirements under GR82 to allow private sector electronic system operators (ESO) to store systems and data outside Indonesia, subject to certain restrictions, GR71 still requires data localization for public sector ESOs.

- In particular, the implementing regulations for GR71, **(Circular 4/2022)** requires public sector organizations to obtain clearance from the ICT Ministry and the Ministry of State Apparatus Utilization and Bureaucratic Reform for any IT procurement to ensure maximum utilization of the state-built National Government Data Center to store data. This requirement presents a challenge for cloud adoption by public agencies, poses additional barriers and operational costs to U.S. cloud services providers, and inhibits the ability of U.S. firms to participate in public sector procurement exercises.

- With respect to the private sector market, while GR 71 previously represented progress towards reforming Indonesia' data localization policy and furthering digital trade, subsequent proposals have set this back by suggesting hard localization mandates through obligations for private ESOs to operate electronic systems and process electronic data in Indonesia. This is quite a hard localization mandate that may be worth flagging in this report, especially as it no longer represents. Further, the developing regime has been undermined by other existing policies that are incongruent with the GR 71 umbrella regulation. For example, data localization policies remain in place for banking and financial sectors. Furthermore, the outgoing government is rushing to revise GR 71 once again, signaling a more regressive policy with more data localization requirements. This includes the Ministry of ICT announcing plans to expand the regulation to include provisions that would mandate companies process and store certain types of data, such as civil registration, immigration, health, and financial data, in Indonesia. The government argues this would be necessary to protect public security. Industry and trade associations like AmCham have been asked to submit input, but to date, the government has not shared the draft revision with the public, and industry reports concern that the new regulations could be passed before the new administration takes office in late October 2024.

- On September 20, 2022, Indonesia's Parliament ratified its **Personal Data Protection Bill**. The bill helpfully differentiates the responsibilities between data controllers and data processors. Data controllers must ensure that any data flows must only go to countries which have equivalent or higher standards of data protection than that available in Indonesia. 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 law also applies extraterritorially if the data transfer has any legal consequences in Indonesia or to its citizens. This applicability covers more processing activities than typically seen in other data frameworks.

- In April 2023, Indonesia's Constitutional Court clarified several ambiguities in the **Personal Data Provision Law** (PDP) following its enactment. The court found that "person" includes legal entities, and they therefore could be data controllers. The court also clarified that PDP applies to non-commercial personal or household activities and that the only processing activities excluded are personal, intimate, non-commercial and/or non-professional. The court also clarified that the contested terms national defense and security is defined through the principle of public interest as defined by prevailing laws and regulations, subject to, for example, relevant regulations like the State Defense Law. which is a justification used in the PDP to limit a data subject's Drafts of implementing regulations of the PDP are under development.

- On August 31, 2023, the Ministry of Communications and Information Technology sought comment on its draft regulation for the implementation of the PDPL that included proposals for cross-border data transfers. The PDPL requires that for data to be transferred to foreign jurisdictions, the data must receive the same protections as they would in Indonesia. The new draft regulations seek to provide entities seeking to transfer data to jurisdictions that do not meet an adequate level of protection to rely on cross-border agreements, standard contract clauses, and enforceable group company rules to do so. The draft regulation is still under consideration.

Japan

- The Japanese Ministry of Communications (MIC) expanded the application of the **Telecommunications Business Act (TBA)** to foreign suppliers of internet-enabled services in 2021, capturing suppliers even if they lacked a juridical presence in Japan. This change mandates that foreign over-the-top (OTT) services, including search, digital advertising, and other services that facilitate communications using third-party facilities to provide notification and register as a local service provider with a local representative, and observe obligations under its Telecommunications Business Act. MIC amended the TBA in 2022 to apply its privacy and data protection obligations to large platform providers and to apply third-party data transfer information—such as the usage of third-party cookies—to all products. Amendments to the TBA implementing requirements for telecommunications providers to disclose a wide array of information to users when transmitting data went into effect on June 23, 2023.

- The **Personal Information Protection Commission (PPC)**, the data protection authority in Japan, has amended the Act on the Protection of Personal Information (APPI) in May 2020, which came into effect from April 2022. The amendments include increased data breach reporting thresholds, stricter data transfer requirements, new standards on pseudonymized personal information similar to the GDPR, and increased data subject access rights with extraterritorial enforcement options. The new cross-border data transfer requirements introduced now require either an individual's opt-in consent prior to the transfer of personal information outside of Japan or an established personal information protection framework with the party receiving the information outside of Japan. The APPI requires a review of the policy once every three years so discussion of revisions are expected to commence in 2023.

Pakistan

- The "**Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021**" was published and enacted by the Ministry of Information Technology and Telecommunication (MoITT) on October 13, 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 defence of Pakistan." Online content providers—such as social media companies—would have 48 hours to comply, failing which the government would have the ability to degrade the providers' services, block the provider, or impose a fine of up to R500 million (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. Local and foreign companies have raised concerns over provisions that would pose significant obstacles to participating in Pakistan's market, including requirements to use mechanisms to monitor and block livestreaming content, take down content within short timeframes when the authorities issue demands, and disclose data to authorities in decrypted and readable formats. These rules greatly jeopardize the ability of U.S. firms to operate in Pakistan and undermine freedom of expression in what is a sizable market.

- The government has repeatedly deployed internet shutdowns in response to protests and elections, imposing large economic losses and harming human rights. Industry has reported that shutdowns have introduced significant uncertainty and encouraged investment flight. In February 2024, a ten hour shutdown of the internet by the government led to an estimated $18.5 million in lost income. In August 2024, local industry began reporting on the government's implementation of an internet firewall to moderate content – triggering widespread network disruptions. According to local industry groups, the firewall has already cost the economy $300 million, with further costs and harms to human rights expected to increase.

South Korea

- Korea's **Personal Information Protection Act of 2011** has always imposed stringent requirements on the transfer of personal data outside Korea, requiring online service providers to provide customers with extensive information about the data transfer, such as the destination of the data, the third party's planned use for the data, and the duration of retention. However, less stringent requirements apply to data transfers to third parties within Korea, which effectively privilege Korean over foreign suppliers in any data-intensive sector without materially contributing to privacy protection,.

- Two years after PIPA's introduction, on May 18, 2023, the Personal Information Protection Commission released amendments for public consultation which aim to reinforce the rights of data subjects by introducing the right to data portability and took effect on September 15, 2023. The amendments provide Korea's Personal Information Protection Commission the authority to impose fines based on global, rather than local revenue. Since most Korean firms subject to this law have negligible foreign sales, such penalties disproportionately affect foreign (and mainly U.S.) suppliers, subjecting them to significantly higher financial risk than their local competitors. This amended law also grants the PIPC the authority to order the suspension of cross-border transfer of personal data based on a generalized risk of breaching privacy protections, absent evidence of specific violations. Such arbitrary authority could affect legitimate personal data transfer by U.S. companies to their U.S. headquarters, jeopardizing significant cross-border trade between Korea and the United States.

- Korea's restrictions on the export of map data continue to disadvantage foreign providers that use such data for services offered in Korea. Foreign-based services providers that offer apps and services that rely on map-based functions—such as traffic updates and navigation directions—are unable to fairly compete against their Korean rivals that generally do not rely on foreign data processing centers and therefore do not need to export map data. Korea is the only significant market in the world

that restricts the export of map data in this manner. Exporting map data requires approval from the Korean government. To date, Korea has never approved the exporting of map data, despite numerous applications by international suppliers. U.S. stakeholders have reported that Korean officials have stated that export approval is dependent on agreement to blur certain satellite imagery of the country--imagery that can be used in conjunction with map data, that Korea seeks to blur ostensibly for security reasons. While competing Korean providers do voluntarily blur select locations at the request of the Korean government, such imagery (provided by third-parties) is readily viewable on foreign mapping services available outside of the country. Thus, it is unclear how restricting the availability and denying the export of such data for foreign suppliers would address the general security concern, since high-resolution imagery of Korea is widely available as a stand-alone commercial product from over a dozen different suppliers. Accordingly, the most logical explanation is that Korea is simply seeking to protect its domestic suppliers from foreign competition.

Thailand

- The **Personal Data Protection Act (PDPA)** went into effect on June 1, 2022, which tracks with some of GDPR, but veers from it with respect to some data transfer provisions. As a general matter, the law 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 creates liability for U.S. online services, as they may be subject to its reach if they decline to establish a business presence in Thailand but have Thai individuals that use their services.

Vietnam

- Vietnam remains a country of concern for industry as it continues to pursue localization measures. The **Law on Cybersecurity**, a key vehicle for localization, took effect on January 1, 2019, and implementation continues through a range of related decrees. The law is expansive and includes data localization mandates, local presence requirements, and content regulations. Under the law, domestic companies, including foreign-invested subsidiaries, are required to store a copy of Vietnamese user data on domestic servers, and to establish a physical presence subject to the jurisdiction of Vietnamese law enforcement. While foreign firms' foreign operations are exempt from these requirements, if the foreign firms' services are used in violation of the law, the foreign firms can be mandated to localize their data.

- On August 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 regarding local data storage and went into effect on October 1, 2022, with no adjustment period. The Decree was issued without Vietnam conducting any consultation regarding the final drafts, which were kept confidential by the government, contravening Vietnam's obligations under in Article 14.13 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP"). The Decree is unclear regarding the scope of localization requirements for domestic and foreign companies; fails to delineate between domestic companies and Vietnamese companies (rendering foreign companies forced to incorporate locally); lacks clarity regarding whether all data sets need to be kept in Vietnam or whether a copy suffices; and includes unclear obligations with respect to local presence and data processing. The Law on Cybersecurity appears to be in conflict with the Location of Computing Facilities (Article 14.13) and Local Presence (Article 10.6) provisions of the CPTPP—implicating the many U.S. companies that are incorporated in CPTPP member countries and that do business in Vietnam.

- The Vietnamese government finalized its **Personal Data Protection Decree (PDP)**, which was issued as **Decree No. 13/2023/ND-CP** in April 2023 and went into effect on July 1, 2023. The Decree prescribes de facto data localization conditions including maintenance of extensive records relating to each individual data transfer and 'registration' of transfer of data of Vietnamese citizens overseas, impacting

cross-border data flows. Given the broad number of service sectors where Vietnam took on full national treatment obligations for cross-border services as part of its accession to the WTO, these restrictions raise serious compliance issues.

- In 2024, the Vietnamese government introduced the draft **Law on Personal Data Protection ("Draft PDP Law")** and draft **Law on Data ("Draft Data Law")**. The Draft PDP Law builds on Decree 13, maintaining a strict consent-first regime, with few exceptions. The draft law would introduce new provisions related categories of data and data assessment requirements and applies vague definitions of "important data" and "core data" that come from China's Data Security Law. These vague definitions would introduce uncertainty and unease among foreign investors in Vietnam that would fear the Chinese model being imported to Vietnam. One significant difference between the Draft PDPL and Decree 13 is that the new draft law would include personal data of all individuals living in Vietnam, regardless of their nationality. The draft Law would also introduce onerous requirements on individuals and organizations to authenticate and assure the accuracy of created data as well as obtaining approvals for the cross-border transfers of important and core data. It also adds specific PDP regulations for various business sectors and types of information, such as marketing activities, targeted advertising service, big data, AI, Cloud computing, monitoring and hiring laborers, financial, banking and credit information, healthcare data, location data, social networks and OTT, biometric data. The administrative burdens for businesses are much heavier than in Decree 13. And the de facto localization requirements from Decree 13 are maintained in the current draft of the Draft PDP Law. The Draft PDP Law may come into effect as early as mid-2025 and industry consultation opportunities may be limited. The Draft Data Law, which is broader in scope than the Draft PDP Law, also applies to overseas entities doing business in Vietnam and includes restrictive data transfer approval mechanisms for certain types of data and worrying obligations to provide data to relevant state agencies when so requested.

Taxation of Digital Services

Australia

- The Australian Taxation Office (ATO) issued a draft ruling in June 2021, dubbed **TR 2021/D4**, that would change the parameters for what is deemed a "royalty" in a manner that if finalized, could implicate digital exporters. The ATO then released an updated version of this ruling that retained the core changes to the treatment of software license distributors, called TR 2024/D1, in January 2024. Although the consultation period ended in June, the final version has not yet been published. Based on this ruling, the delivery of software could be subjected to Australian withholding tax as a royalty and has been considered by the ATO as part of this update. This change to Australian tax code splits from both prior practice in the country and international norms. Under Australia's previous code TR 93/12, which stood in place until the introduction of the new proposal, distributors of software licenses were not deemed to be paying royalties for payments if the license was made to end-users to ensure no software copyrights were being violated. The OECD Model Tax Convention on Income and on Capital similarly recognizes this right, stating that "distributors are only paying for the acquisition of the software copies. The new approach, under TR 2021/D4, would classify distributors and resellers as engaging in an ancillary "authorization" copyright inherent in software programs, regardless of whether the owner of the software copyright has approved any rights to modification, reproduction, or other actions to the distributor in question. This would subsequently implicate traditionally typical aspects of a transaction between software distributors and resellers in engaging in copyright rights exchanges rather than simply exchanging a copyrighted article or supplying a service. Industry is concerned that in its current form, TR 2021/D4 fails to separate income tax applications on payments for gaining copyrighted software and those made to exploit copyright rights. The direction of the rules contravenes international norms on the taxation of software rights and payments that have persisted for years, which could have consequences for U.S. and global firms in Australia and internationally if other jurisdictions similarly abandon precedent. Particularly concerning for U.S. companies, the ATO does not see TR 2021/D4 as inconsistent with its Double Taxation Avoidance Agreements, including its DTAA with the United States.

India

- In 2016, India imposed a 6% withholding tax on the provision of digital advertising services provided by non-residents to Indian residents. This equalization levy was based on gross revenue generated from online advertising services, not profits, deviating from established international tax principles. It also led to double taxation, as it was introduced outside the Double Taxation Avoidance Agreement, with no credit available. In 2020, the government added a 2% equalization levy on consideration received by non-resident e-commerce operators, largely scoping those selling digital services, digital advertisements, and data. USTR subsequently investigated the 2% equalization levy and found it actionable under Section 301. While the Indian government repealed the 2% equalization levy as of August 1, 2024, the 6% equalization levy remains in place.

Indonesia

- Indonesia issued Regulation **No.17/PMK.010/2018 (Regulation 17)** in 2018. The Regulation amends Indonesia's Harmonized Tariff Schedule (HTS) Chapter 99 to add: "Software and other digital products transmitted electronically." This makes Indonesia the only country in the world that has added electronic transmissions to its HTS. This unprecedented step laying the groundwork to imposing customs requirements on purely digital transactions will impose significant and unnecessary compliance burdens on nearly every enterprise, including many SMEs. While the tariff rate is currently specified as zero, the policy conflicts with Indonesia's commitment under the WTO's moratorium on customs duties on electronic transmissions, dating back to 1998 and most recently reaffirmed in June 2022. Left unchecked, Indonesia's actions will set a dangerous precedent and may encourage other countries to violate the WTO moratorium. Further, viewed in tandem with Regulation No. 190/PMK.04/2022, Indonesia's actions are deeply concerning to industry, as it appears to be the beginnings of a regime to impose and collect customs duties on electronic transmissions. This is especially critical as members at the WTO continue discussions on e-commerce, and as the renewal for the moratorium comes up during the 14th WTO Ministerial Conference expected to occur in 2026. Given the threat Indonesia's policy poses to the future of the WTO agreement. Indonesia must rescind Regulation 17 and remove Chapter 99 from its HTS.

- In March 2020, Indonesia introduced tax measures targeting digital services as part of an emergency economic response package. One of these taxes applies to e-commerce transactions carried out by foreign individuals or digital companies with a "significant economic presence" in Indonesia. Significant economic presence will reportedly be determined through the companies' gross circulated product, sales and/or active users in Indonesia. Companies determined to have a significant economic presence will be declared permanent establishments and as a result subject to domestic tax regulations, a departure from long-established international tax principles. This definition of permanent establishment could conflict with existing tax treaties, including with the United States, resulting in a new "electronic transaction tax" (ETT) applying to income sourced from Indonesia. While structurally different from digital services taxes adopted in some European countries, the tax is similarly concerning insofar as it looks to unilaterally increase U.S. firms' tax payments in the region by departing from longstanding international taxation norms, while also basing application of the tax on arbitrary distinctions between digital and non-digital companies competing in the same consumer markets. U.S. companies were cited as targets of these tax measures, and industry reports that this tax in effect only applies to non-Indonesian entities, reflecting a discriminatory taxation regime. Indonesia's designation of foreign companies with significant economic presence as permanent establishments contradicts international norms of determining permanent establishment and creates a significant barrier for cross-border suppliers.

- A new VAT on digital goods and services went into effect on April 1, 2022. The VAT will be collected on all goods and services that are taxable and delivered to Indonesia via electronic systems at a rate of 11% (which will rise to 12% starting in 2025).

- Industry reports that Indonesia continues to act in violation of its WTO tariff binding for a set of imported technology products that should benefit from duty-free treatment under the commitments made by Indonesia to the Information Technology Agreement (ITA). Thus far, Indonesia only introduced ITA commitments for five categories of goods/HS codes (Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods). Even within those categories, however, Indonesia has reclassified certain technology goods with similar functions into dutiable HS codes that would fall outside these 5 categories, as a method of increasing revenue. Examples of this include Indonesia's continued practice of applying duties for printers and related parts, equipment for data centers and for connectivity (such as routers, switches, servers and server racks, optical modules, and optical cables), solid state drives, among other ICT products, all of which are covered by the ITA. In the view of industry, the reclassified HS codes should be protected by Indonesia's ITA commitments. By raising import costs, this practice broadly harms the IT industry and imposes burdens on U.S. investors and their workers alike.

Nepal

- Nepal passed legislation on May 29, 2022, that would implement a 2% digital services tax (DST) to be collected from a specified list of digital services provided by non-residents to users in Nepal. The DST took effect on July 17, 2022, without any public consultation on the law itself or the procedures implementing the tax. The DST applies exclusively to non-resident companies; contradicts existing international tax principles; creates an additional burden of taxation with the potential of double taxation for non-resident companies; and establishes a disproportionate compliance burden for U.S. and other foreign companies due to the additional resources needed to comply with the DST's payment and reporting obligations.

- In 2024, Nepal adopted a new amendment called the "Significant Digital Presence tax," which stipulates that "a place where a person or entity, while residing outside Nepal, demonstrates significant digital presence in Nepal or a place where data or service business is carried for at least ninety days within the past six months using servers located outside is required to pay an additional 5% tax on repatriation of profit to non-resident parent company." This 5% tax is imposed on foreign tech companies along with the 2% DST and 5% VAT. This tax will be in force in January 2025.

New Zealand

- On August 31, 2023, the government introduced a **Digital Services Tax Bill** that would empower the government to introduce, at an appropriate time, a 3% tax on gross revenues of large international firms with digitalized business models that earn revenue in New Zealand. The effective date is expected to be January 1, 2025, which could be extended by an Order in Council if the government deems the progress of the Pillar One of the OECD's multilateral solution to be adequate.

Philippines

- The United States and the Philippines are party to the **Income Tax Convention of 1976**, which is now in force between the two nations. This treaty ensures that a country's taxation of the profits of a business earned by a resident of the partner country is overseen by the "standard treaty concept that tax liability will arise only to the extent that the profits are attributable to a 'permanent establishment' in the taxing country." Implementation of this treaty, however, has been challenging. The Bureau of International Revenue (BIR) requires income tax payors to apply for status under this treaty, approval which is governed by complex and burdensome documentation procedures. Failure to adhere to the documentation guidelines can lead to entities being subjected to penalties and criminal liabilities. The BIR has not established standard processing timelines, and businesses are subsequently required to wait indefinitely without any commitment towards a resolution of the filing. These requests are required of all

U.S. non-resident service providers operating in the Philippines and, therefore, this policy is not limited to digital services and impacts members of all industries seeking to provide their services and goods to the Philippines market.

- The BIR's issuance of **Revenue Memorandum Circular No. 5-2024 (RMC)** in January 2024 added further confusion to income-tax obligations of non-resident suppliers of cross-border services. The RMC appears to depart from established principles of income taxation of cross-border services (using the place where the services are performed to determine if the transaction is income-taxable) and treats the place of receipt of the services as being crucial in determining the taxability of the transaction. The BIR and the Philippines government should engage in comprehensive industry consultation, including with U.S. non-resident service providers, to clarify the income-tax position under Philippines law in line with well-recognized and established international practices.

- The Philippines government has adopted a new law **(RA 12023)** to impose a 12% value-added tax (VAT) on digital services consumed in the Philippines and provided by both resident and non-resident digital services providers (DSPs). The digital services included within the scope of this measure are online search engines, online marketplaces or e-marketplaces; cloud services; online media and advertising; online platforms; and digital goods. While this law imposing VAT on DSPs does not discriminate between U.S. non-resident DSPs (or other foreign DSPs) and local DSPs, industry is concerned that implementing rules and regulations, which are currently being developed, could impose unworkable requirements on foreign DSPs similar to what has happened above for income-tax payors. The Department of Finance (DOF) and BIR are expected to develop the Implementing Rules and Regulations (IRR), with the expectation for the start of the implementation of the law and collection to be in 2025.

Vietnam.

- The **Tax Administration Law**, effective July 1, 2020, taxes cross-border e-commerce and other digital services. The Ministry of Finance issued Circular 80 providing guidance on Law on Tax Administration and its Decree 126 in September 2021. The Circular added a requirement for foreign digital service/e-commerce suppliers without a permanent establishment in Vietnam to directly register and pay tax to the tax authorities. If the foreign service providers do not register, service buyers (or commercial banks in case of individual buyers) will withhold tax from their payment to foreign suppliers at deemed tax rates. The legislation allows digital suppliers to seek exemptions under bilateral tax treaties but the process for obtaining such benefits remains unclear. This onerous procedure coupled with the deemed tax rates (Corporate Income Tax and Value Added Tax) will further complicate tax obligations for cross-border service providers and conflict with international taxation rules.

Asymmetric Platform Regulation

Australia

- The Australian Competition and Consumer Commission released a consultation seeking comments on a set of reforms in December 2022 to adopt a "new regulatory framework for consumer protection and to improve competition." The ACCC puts forward a series of recommendations, with parallels to the EU DMA, including "targeted obligations" regarding "anti-competitive self-preferencing;" "anti-competitive tying;" "exclusive pre-installation and default agreements that hinder competition;" "impediments to consumer switching;" "impediments to interoperability;" "data-related barriers to entry and expansion, where privacy impacts can be managed;" "a lack of transparency;" "unfair dealings with business users;" and "exclusivity and price parity clauses in contracts with business users." Mandatory processes for scanning for "scams, harmful apps and fake reviews" are among the recommendations as well. The ACCC accepted comments through Feb. 15, 2023, and on April 28, the ACCC released the sixth interim report for the Digital Platform Services Inquiry. Industry remains concerned that the final recommendations from the ACCC focus on ill-defined and poorly documented harms, the implementation

of which will hinder the competitive delivery of services by U.S. digital suppliers in Australia. This initiative represents another instance of a country following the EU's lead in furthering unproven, experimental regulation without careful consideration of their unintended consequences.

- On August 23, 2024, the ACCC concluded a public consultation on competition and consumer issues in digital platforms services. The consultation will feed into the Commission's inquiry into digital platforms services, focused on regulatory developments and their impacts, distribution and subscription models, and competition issues related to generative AI. The consultation follows the Commission's release of interim report 8 in the government's "Digital platform services inquiry," with initial findings that platforms provide insufficient transparency and choice to consumers regarding personal data.

- A November 2023 proposed rule Australia is considering would empower its central bank with overly broad authority to oversee digital payment providers like Apple Pay and Google Pay. If implemented, the draft law would expand the definitions of "payment system" and "participant," and introduce "a new ministerial designation power that will allow particular payment services or platforms that present risks of national significance to be subject to additional oversight by appropriate regulators."

- In October 2024, the ACCC submitted initial comments in response to Treasury's consultation on Revitalizing National Competition Policy, in which the agency argued that digital services providers with identified monopoly characteristics should be subject to the same broader regulatory framework as monopolies controlling physical infrastructure such as rail networks and ports. The ACCC posited that regulatory uncertainty related to the application of existing infrastructure access rules to digital services has created a series of industry-specific siloed frameworks, rather than an overall regime. This begs the question of whether market dynamics in sectors as different as software-defined industries and physical infrastructure justify a common regulatory approach.

India

- On December 22, 2022, an Indian parliamentary panel recommended that India adopt a "**Digital Competition Act**," which would include European Digital Markets Act-like ex-ante regulations for "systemically important digital intermediaries." The proposed rules appear to be largely targeted at U.S. tech companies. The panel gave recommendations on a range of DMA-inspired rules for select market participants, relating to, inter alia, anti-steering practices; platform neutrality; bundling and tying; data usage; mergers and acquisitions; deep discounting; exclusive tie-ups; search and ranking; restricting third-party applications; and advertising policies.

- In October 2022, the Competition Commission of India issued far-reaching orders seeking changes to how the Android operating system and the Google Play store function in India. While ostensibly seeking to address competition issues, the order, which is under appeal, may lead to a fragmented, more expensive and less sustainable market for applications, introduce interoperability problems and significantly increase cybersecurity risks in the mobile ecosystem.

- In 2024, the Indian government released a draft **Digital Competition Bill**, an ex-ante regulatory framework aimed at preventing systemically significant digital enterprises from engaging in presumptively anticompetitive behavior. In March 2024, the Committee on Digital Competition Law submitted the draft report to Parliament, and the government is now engaging with industry stakeholders.

Japan

- On July 5, 2022, the Ministry of Economy, Trade and Industry released a Cabinet Order which stipulated that the digital advertising sector would be regulated under the 2020 **Act on Improving Transparency and Fairness of Digital Platforms (TFDPA)**. Platforms that use advertisers' ads on their websites—such as search engines, portal sites, and social networking services, primarily through auctions—would

be designated under this new policy if they sell at least 100 billion yen (roughly $691.4 million) each fiscal year in Japan. Platforms that serve as intermediaries between advertisers and website operators primarily through auctions would be designated if they sell at least 50 billion yen (roughly $345.7 million) each fiscal year in Japan. An intent to target U.S. firms is evident in the Final Report on the Evaluation of Competition in the Digital Advertising Market by the Digital Market Competition Council—which set the foundation for these new rules—which identified only Google, Facebook, and Yahoo! in its analysis of the market. In February 2024 METI released its first major review of compliance with the new law, evaluating the practices of 6 companies, four of which were U.S. multinationals. Based on this review, METI called on the targeted companies to "strive to improve their operations" or face "certain [unspecified] measures," authorized under the TFDPA (e.g., a ministerial recommendation to "promptly cease its disadvantageous treatment" (Article 10). To date, no such recommendations appear to have been issued.

- In June 2024, Japan's Diet passed a law proposed by the DMCH to address allegedly unfair practices in the mobile market ecosystem. The law, entitled "**Act on Promotion of Competition for Specified Smartphone Software**" (SSCPA) was promulgated June 19 and will take effect no later than the end of 2025. Enforcement of the law will fall to the Japan Fair Trade Commission (JFTC) which is currently in the process of developing implementing regulation. A public notice and comment process is ongoing. Although scoped more narrowly than the EU's Digital Markets Act (DMA), this law, like the DMA it draws inspiration from, is intended to target the two U.S. firms active in the mobile ecosystem in Japan. Statements by legislators to this effect, during the passage of the law, are likely to be formalized when the process of designation (i.e., name the specific companies subject to the ex ante obligations of the law) occurs next year.

- For designated companies, the SSCPA seeks to prohibit, on an ex ante basis, 13 forms of conduct, almost all of which have parallels with the DMA. Included among prohibitions are practices relating to tying (bundling of services), to self-preferencing (providing advantages to self-owned products or services) technical interoperability, use of commercial data, default settings, service portability, and third-party sellers ability to communicate with their customers. Since these practices are common across many industries, and in many cases have strong consumer welfare effects (e.g. consumer convenience, efficient pricing, protection of privacy and preventing malware), the presumption that they are or are likely to be anticompetitive, and that their use could result in harms, is unjustified. Although the SSCPA provides greater leeway than the DMA for a company to defend practice that might otherwise run afoul of the prohibitions, the presumption against such practices, in addition to having questionable benefits to competition is likely to incur significant compliance costs on U.S. suppliers. As Japan begins moving to designate specific companies, it will be important for authorities do so fairly consider competing local or third-county suppliers, several of which have competing products or services that will be accorded an advantage if shielded from similar burdens.

- Japan should also reconsider the broader policy of identifying a market so narrowly as to intentionally capture specific U.S. companies while exempting local competitors, both in the mobile ecosystem and in parallel markets. Although one of the stated intents of the law is to create more competitive digital marketplaces, other digital markets in Japan, dominated by Japanese suppliers, have not been similarly regulated although many practices mirror those the SSPCA seeks to prohibit. For example, the console gaming market has long been dominated by Sony, which enjoys, by one metric, a market share of over 90 percent. Like U.S. suppliers of mobile apps, Sony also operates a "walled garden" game store, requires commissions on games equal to those of app stores, and prohibits the use of alternative payment systems. Since mobile apps often compete against such games, subjecting U.S. firms to onerous prohibitions while exempting a competing Japanese supplier is an obvious example of discrimination that raises serious trade rule concerns — e.g., Japan's National Treatment and MFN commitments with respect to distribution services. Although U.S. officials have been loath to criticize any measure ostensibly pursued in the name of competition, this is a clear example of where a more thorough examination of the motivations and effects of a measure is called for.

South Korea

- In July 2024, Representative Kim Nam-geun and several dozen other Korean National Assembly representatives introduced the **Online Platform Monopoly Regulation Act**, one of a number of bills that would impose sweeping restrictions to online services providers' offerings to consumers. The bill targets firms based on arbitrary criteria (e.g., firms with an average market capitalization of at least KRW 15 trillion (approximately $11 billion), annual revenues of KRW 3 trillion (approximately $2.2 billion), and 10 million monthly users or more) and restricts these companies' ability to offer products that self-preference or engage in tie-in sales, whereby a firm promotes its own or affiliated products or services. The bill also envisages requiring mandatory data sharing (e.g., search results for products distributed through a platform), a requirement that raises trade secrets concerns and thus Korea's commitments under the WTO and KORUS. Although some South Korean companies would be scoped into the bill's reach, the law would disproportionately hinder U.S. service providers' ability to operate in the market, while sparing similar services in other sectors where Korean suppliers are prominent in the domestic market (brick and mortar stores vs. e-commerce, search engines and mapping services vs. auto manufacturers and mapping services, and social media services vs. rival communications services, to name a few). Meanwhile, many Chinese and Russian companies, based on current criteria, would be left out of scope, thereby giving them preferential treatment in the Korean market, and access to competitors' data that could pose security risks.

- This legislation would likely cause unintended harm to Korean businesses and consumers. As the bill appears to replicate the approach of the EU's Digital Markets Act in prohibiting self-preferencing (a practice common in a wide variety of industries both digital and traditional), digital providers would be impeded in developing innovative product pairings that users find helpful. For example, the smartphone and its integration of dozens of services that used to be sold separately—such as voice services, text messaging/paging, music, GPS, email, a clock, calculator, etc.—is a prime example of the types of product integrations that could be prohibited under the legislation.

- Meanwhile, the Korean Fair Trade Commission (KFTC) has been developing a similar legislative proposal of its own, but in the face of strong opposition from both Korean and U.S. firms, academics, and at least one Korean agency (MSIT), it announced, in September 2024 a revised approach ostensibly moving away from ex-ante regulation in favor of a prescriptive enforcement framework. The proposed amendment aims to prohibit, for select operators, self-preferencing, tying sales, restrictions on multi-homing, and requiring sellers to offer "most-favored-nation" treatment. To help enforce these prohibitions, the amendment will shift the burden of proof onto targeted platforms (i.e., so they must prove that their actions are not anticompetitive) and increase the penalties for violations, including fines of up to 8% of related sales revenue and the possibility of provisional suspension orders. The amendment allows platform operators a defense, if they can demonstrate that their actions are not anti-competitive or are necessary for data protection or security. However, the premise of this proposal is the existence of presumptively anticompetitive conduct, applicable only to a subset of market participants. While th9is represents an incremental improvement over competing bills, the KFTC's new ex-post framework still includes discriminatory thresholds and "gatekeeper" definitions seen in competing bills. In developing this proposal there has been a troubling lack of transparency and industry is concerned the process has featured inadequate opportunity for consultation. The KFTC has not published any impact assessments that demonstrate likely effects of its proposal or the necessity of such legislative changes. Moreover, the KFTC has not conducted outreach to the business community through public consultations or hearings.

- Both the KFTC proposal and competing bills allow a targeted company try to prove that proscribed conduct is welfare-enhancing or is necessary for business reasons, but the burden of proof countering this presumptively anticompetitive conduct is placed on the targeted company. Given that burden, and the heavy fines that can result from an adverse finding, the chilling effect of these bills is obvious.

- Both these approaches continue to target U.S. firms and put them at a competitive disadvantage as vis-a-vis a broad range of Korean companies offering similar services. By targeting U.S. companies through arbitrary thresholds, and proscribing conduct competitors are free to engage in, both approaches reflect protectionist competition policy and are potentially inconsistent with Korea's international trade commitments, including under the Korean-U.S. FTA (KORUS).

Taiwan

- On July 12, the Legislative Yuan passed the draft **Fraud Crime Harm Prevention Act**, the Technology Investigation and Protection Act, and related legislation to advance anti-fraud measures in the digital economy. Under the draft Acts, select online advertising platforms and e-commerce operators will be subject to new anti-fraud obligations. The Fraud Crime Harm Prevention Act raises particular concerns given the lack of due process in the drafting process and the significant burdens it places on digital platforms. The Act was pushed through the drafting process without sufficient consultation opportunities, bypassing the conventional 60-day review period. As a result, stakeholders were unable to provide meaningful input on the Act's practicality and compliance requirements. The Act also imposes serious burdens on industry, including greater oversight from the Ministry of Digital Affairs, stringent verification and disclosure requirements regarding advertisers on their platforms, and regulations on the use of generative AI in ads. These obligations appear to disproportionately target a small group of just four major companies: two American, one Japan, and one Chinese. This rushed legislative process and burdensome requirements could act as a non-tariff trade barrier, discouraging foreign investment and participation in Taiwan's digital economy.

Thailand

- The **Royal Decree on Digital Platform Services (B.E. 2565)** came into effect on August 20, 2023, and requires relevant services to notify the government prior to starting business operations, with large-scale services subject to additional requirements such as mandatory risk management systems and internal compliance managers. The Decree is overly broad beyond the authority of the government and does not recognize different platforms' business models. It also imposes burdensome obligations and liabilities on businesses, such as local representative with unlimited liability, reporting requirements, and broad authority for ETDA to further prescribe any additional requirement in the future. The Royal Decree sets out a requirement for each operator to have a Code of Conduct which includes users and advertisers' merchant ID verification, but has failed to provide further details, creating uncertainty. Industry reports the government is considering making verification mandatory.

- Thailand announced its intention to develop a **Platform Economy Act** in January 2024. The Draft PEA seeks to regulate and standardize digital platform service business operations. Once the Draft PEA becomes law, it will supersede other existing law, such as the **Royal Decree on the Operation of Digital Platform Service Businesses** that are subject to **Prior Notification B.E. 2565** of 2022 and the relevant provisions under the **Electronic Transactions Act B.E. 2544** of 2001. The Draft PEA reflects strong influences of the EU's Digital Services Act (DSA) and Digital Markets Act (DMA).

Uzbekistan.

- In May 2024, Uzbekistan published a regulation on designating digital platforms with either a dominant position or superior bargaining power ("**Resolution N256**"). The rules include ex-ante obligations for digital suppliers in the same manner as the EU's DMA.

- The list of regulated platforms and ex-ante obligations is more extensive than those in the DMA and include new categories such as AI-based platforms that could undermine the growth of digital services, the development of local AI systems, and the ability of companies generally to "operate fairly". Industry

reports a concerning lack of transparency in Uzbekistan's lawmaking process, offering companies insufficient opportunity to provide feedback. The lack of transparency and consultation with the business community for this set of rules reflects the broader challenges observed by the U.S. government in documents such as the State Department's Investment Climate Statement for Uzbekistan.

- Industry urges engagement with Uzbekistan to redirect Uzbekistan's approach away from discriminatory measures and to instead align with non-discrimination ideals that would improve business conditions and cross-border trade.

Threats to the Security of Devices and Services

Australia

- The Australian Parliament passed the **Telecommunications (Assistance and Access) Act** at the end of 2018, granting the country's national security and law enforcement agencies additional powers when dealing with encrypted communications and devices. The legislation authorizes the Australian government to use three new tools to compel assistance from technology companies in accessing information within electronic communications. These tools are technical assistance requests (TARs), which seek voluntary assistance from communications providers; and technical assistance notices (TANs) and technical capability notices (TCNs). These tools call upon providers to do one or more specified acts which could include building new technical capabilities as required by the Attorney General. While the legislation specifically forbids a notice to provide a "systemic weakness or vulnerability" into an encrypted system, it provides authority to undermine encryption through other technical means with little oversight. The Australian Government Department of Home Affairs disclosed in a February 2022 report that New South Wales Police was granted a TAN for the first time, empowering the agency to "compel designated communications providers to give assistance where they already have the technical capability to do so."

- In April 2022, Australia passed the **Critical Infrastructure Protection Bill 2022**. The proposed legislation significantly expands the sectors considered critical infrastructure (including companies that provide "data storage or processing" services) and will impose additional positive security obligations for critical infrastructure assets (e.g. risk management programs and cyber incident reporting), enhanced cyber security obligations and, most concerningly, government assistance measures that would enable Australian government agencies to require critical infrastructure entities to install monitoring software on their networks, to 'take control' of an asset or to follow directions of the Australian Signals Directorate.

Hong Kong

- In 2022, the Hong Kong government announced a plan to introduce a bill to strengthen the cybersecurity of critical information infrastructure in Hong Kong. On June 25, 2024 the government published a new draft **Protection of Critical Infrastructure Bill**. The Bill includes the category of "information technology and communications", and imposes new requirements for preventing and reporting cybersecurity incidents. This category is overly broad and risks scoping in companies that are in no way relevant to the core issue of critical infrastructure protection. The draft continues to contain extensive investigatory powers for the government, drawing widespread criticism from commercial entities concerned that the law would provide the Hong Kong government unprecedented access to their systems. The bill also has extraterritorial aspects and could allow government demands to infrastructure and systems of companies outside of Hong Kong. The draft also includes authority for the Commissioner's Office to connect equipment to or install programs in critical computer systems of critical infrastructure operators (which can be a wide range of digital services providers, under the definitions of the bill). AmCham Hong Kong describes the implications as follows: "Such unprecedented power directly intervenes in, and could have a significant impact on, a CIO's operation and could harm the users of the services provided by the CIO.

Moreover, as such power might be exercised within a third-party service provider's environment, it could further interfere with the operations of the third party, create potential vulnerabilities and weaknesses, and cause the third party to breach its contractual arrangements with its customers or to violate any applicable laws." The bill is likely to be approved by the Legislative Council by the end of 2024.

South Korea

- In late 2022, in response to a fire at a major data center, the National Assembly passed the amendments to the **Broadcasting Communications Development Act ("BCDA")**, the **Telecommunications Business Act ("TBA")**, and the **Act on the Promotion of Information and Communications Network Utilization and Information Protection ("Network Act")** to encourage resiliency of data centers. The legislation entered into force in July 2023. Among the requirements of this law are extensive demands for data related to data center security that could jeopardize companies' cybersecurity and nondisclosure agreements, and making sensitive data related to infrastructure, security, and commercially sensitive trade secrets vulnerable to exposure.

Potential Challenges to the Development of AI

Australia

- On 5 December 2023, Australia's Attorney-General announced the establishment of a **Copyright and Artificial Intelligence Reference Group (CAIRG)** to better prepare for future copyright challenges emerging from AI.

- The Australian Department of Industry, Science, and Resources (DISR) is pursuing a regulatory framework that would establish mandatory guardrails for high-risk AI systems, as first proposed on September 4, 2024. Despite the framework's intended interoperability with other national regulations, it advances broad principles for AI governance that would impose substantial burdens on the private sector. In particular, industry remains concerned that it does not clearly define which AI systems are considered high risk according to a specific threshold of potential harm, instead defining all general-purpose AI systems as high risk. Given U.S. companies' leading edge in AI innovation, such a broad scope would mostly capture U.S. companies, imposing substantial disclosure obligations disproportionate to the risk their systems pose.

Japan

- The Japanese government is also now considering binding AI regulation, based on a proposal by a government working group for a **"Basic Act on the Advancement of Responsible AI" ("Basic AI Bill")**. The proposed Basic AI Bill would designate AI systems and developers subject to regulation and impose safety obligations and transparency requirements relating to the vetting and operation of the systems, and periodic reporting on the systems. The law is expected to be similar to the US White House AI Commitments as well as the White House Executive Order on AI. The draft bill could be submitted to the Japanese Diet as early as next year, with the law expected to be approved by the June 2025 session of the Diet. Similar to the concerns in relation to the SSCPA, it would be imperative to ensure that the Basic AI Bill and any policy or regulation that the Japanese government may adopt to regulate AI in future does not unfairly target or discriminate against U.S. firms.

South Korea

- On February 14, 2023, the National Assembly Science, ICT, Broadcasting and Communications Committee advanced the "**Law on Nurturing the AI Industry and Establishing a Trust Basis**," following 12 different bills related to artificial intelligence that have been introduced in the previous three years.

While the bill does not discriminate based on nationality or size, it includes increased and unclear obligations on systems of AI determined to be "high-risk," including methods for detailing how an AI system reaches its final decision. The broad classification of what constitutes high-risk is comparable to that of the EU AI Act and could envelop more services than appropriate.

Vietnam

- In July 2024, the Vietnam government released the draft **Digital Technology Industry Law**. The draft bill includes concerning mandates such as access and portability obligations that are technically impossible with no safeguards. Additionally, AI developers would be required to monitor the down-stream use of their technology and services, for which company compliance would be extremely infeasible.

- Further, the bill also includes an overly broad and vague provision that details what could be viewed as prohibitions on the development or deployment of any AI technology (e.g. Article. 7). For example, the broad definition of "digital technology" could include diverse and rapidly evolving technologies such as artificial intelligence (AI), big data, and blockchain, which industry is concerned could lead to overly-prescriptive regulations. This is, in part, due to the draft law's focus on prioritizing investment, lease, and procurement of domestically produced digital technology products and services, which could result in unfair treatment of foreign competitors, and U.S. businesses in particular that are leaders in this space.

- Overall, the regulator is given sweeping oversight authority with inadequate guardrails that could empower undue and subjective interpretation (such as defining what constitutes an activity that "violates morality" or "causes adverse effects on social security of individuals in Vietnam"). This article threatens to result in unpredictable or unfair enforcement for companies.

- As currently drafted, this Article might also potentially censor speech and expression on the internet relating to what systems can use to train services and what consumers can enter as prompts, while also furthering biases in the outputs of GenAI services.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

India

- In September 2022, the Department of Telecommunications released the **Draft Indian Telecommunication Bill**, which updates and aggregates the Indian Telegraph Act of 1885, the Indian Wireless Telegraphy Act of 1933, and the Telegraph Wires (Unlawful Protection) Act of 1950. On December 24, 2023, the President of India signed the Telecommunications Bill 2023 into law. Many provisions of the Bill overlap with existing provisions in the IT Act and Digital Personal Data Protection Act, including those relating to lawful interception and blocking content, privacy and security, customer verification, and consumer grievance redressal. It is also unclear how it will interact with forthcoming legislation such as the **Digital India Act**.

- The legislation would redefine "telecommunication 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. The bill carries a broad definition of telecommunication services, which would include over-the-top (OTT) services, user-to-user communication, and cloud services. Broad definitions of "messages" and "telecommunications" could additionally subject a wide range of internet-based services and digital communication services to the law, with insufficient clarity included in the text of the law.

- The language further suggests all players in the communication space that provide "telecommunication services" would require authorizations, which would mean that all covered services are now reliant on government approval, unless they have been otherwise exempted. The law also suggests that approvals

would be required for setting up telecommunication networks, including infrastructure for providing telecommunication services, which, for internet-enabled services, would include data centers. The bill stipulates that this new, broadly-defined category of "telecommunication services" would be required to pay fees associated with obtaining authorization. Similarly, the Bill mandates fee payment to the Universal Service Obligation Fund. This could mean that if internet services are determined to fall within the ambit of telecommunications services, they would be obligated to dedicate funding to a public fund in India without being able to access the fund themselves, given they are not telecommunications infrastructure operators. Such a regime gives a preferential benefit to Indian local telecommunications suppliers that may also be required to contribute to the fund but are able to access the funds.

- The law carries concerning provisions relating to consumer privacy and government overreach as well. The Bill imposes obligations of "biometric verification" on all authorized telecommunication service to ensure that sensitive biometric information is analyzed and stored. Depending on how implemented, this requirement could undermine user privacy and potentially imposes significant operational compliance costs on service providers. Other onerous obligations include licensing requirements; government access to data; encryption requirements; support for internet shutdowns; liability for seizure of infrastructure; and additional monetary obligations for the sector. Such obligations are likely to undermine digital security and freedom of expression and will impose one of the world's first general licensing regimes for internet-enabled service suppliers.

- A key aspect of this law is the troubling move of authority away from the traditional regulator, TRAI, to a central government authority. Depending on how the bill is implemented and enforced, the legislation could contravene India's WTO commitments under the GATS. While many India-based services will be subject to the regulations, U.S. companies are likely to represent the majority of internet-based services impacted by the law.

- A TRAI consultation paper released in July 2023, "Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services," also put forward similar proposals to impose telecommunications licensing obligations onto internet-enabled services. Among the questions posed by TRAI was whether a "collaborative framework" between OTT providers and telecommunications infrastructure providers would be necessary, evoking similar language to the "network usage fee" debate that has gained momentum in India.

Nepal

- In March 2022, the Nepal amended its **National Broadcasting Rules 2052** to require broadcast OTT, video-on-demand (VOD), and online television services in Nepal to obtain broadcast licenses from the Ministry of Information and Communications before being able to serve the local market. Additionally, Broadcast OTT providers will need to maintain local cache servers in Nepal, store user data and program records for at least 60 days, and adopt age-based categorization of Broadcast OTT content.

- In April 2023, the Nepal Telecommunications Authority (NTA) released a draft framework to regulate voice/video telephony and messaging over-the-top services ("Communications OTT"), which would require Communications OTT providers to obtain an authorization from NTA before providing their services in Nepal. To obtain the authorization, Communications OTT providers will need to register a branch office or appoint a local intermediary in Nepal.

- These changes to the broadcasting and telecommunications regulatory regime in Nepal create significant regulatory and financial burdens on U.S. and other countries' Broadcast OTT, Communications OTT, VOD, and Online TV providers seeking to serve the Nepal market.

South Korea

- The Ministry of Science & ICT has promulgated regulations made pursuant to amendments to the **Telecommunications Business Act passed in 2020**, imposing obligations on OTT suppliers, including foreign suppliers, for network management issues outside their control, ostensibly to mitigate network congestion.651 The rules subject predominantly U.S. internet services to disproportionate levels of risk and responsibility regarding network management over which they have no control.

- The rules inappropriately shift the burden for network management to "value-added telecommunications service providers" (VTSPs), even though they lack the technical or information capabilities to control end-to-end delivery of the content. Internet service providers who control the network infrastructure remain the most relevant to service reliability. These changes could also lead to unbalanced bargaining positions resulting in discriminatory or anti-competitive behavior by ISPs to the detriment of VTSPs, which could lead to demands for increased usage fees or other contractual conditions.

- Eight proposals have been made by the Korean National Assembly to explicitly mandate "network usage fee" payments by certain content providers over the past several years. A new legislative proposal from Representative Lee Hae-Min, dubbed the "**Bill on Partial Amendment to the Telecommunications Business Act**" and which amends the Telecommunications Business Act, was introduced on Aug. 8. The bill prohibits value-added telecommunications service providers that meet certain user and data traffic thresholds from, among other requirements, unjustly delaying or declining to enter into a contract for the use of telecommunications networks or declining to pay a "legitimate" price for the use of telecommunications networks. This contravenes the free-market system based on voluntary negotiation that has allowed the internet to flourish—with vast benefits to online services and telecommunications providers alike—by allowing telecommunications providers to force value-added services providers to pay fees for their traffic. Proponents justify such proposals with the unsupported argument that network fees are necessary to fund the costs of extending and adding capacity to local broadband markets. However, in reality, such a regime would distort investment incentives and lead to discriminatory treatment of content and application providers.

- Such proposals can be traced to years of conflict between U.S. content providers operating in the region and local telecommunication providers, culminating in legislation introduced in 2022 by Rep. Young-chan Yoon, called the "**Netflix Free Ride Prevention Act.**" The legislation would effectively mandate foreign content access providers—namely U.S. firms such as Google, Meta, and Netflix—to enter into paid contracts with internet service providers for the content demanded by ISPs' customers. The bill would directly undermine long-standing global norms and procedures that serve as the foundation of the internet ecosystem and would likely violate Korea's trade obligations to the United States by targeting U.S. content providers and requiring contracts and extractionary fees for any company meeting arbitrary data transfer thresholds. In addition, the bill would have a detrimental impact on the domestic content industry by increasing the cost for users to access content and inhibit the overseas expansion of K-content. Korea's existing Sending Party Network Pays (SPNP) model, adopted in 2016 and applicable to ISPs operating in Korea, demonstrates that these concerns are not merely speculative. Multiple studies have found that Korea's SPNP model has led to higher transit prices, higher latency, and high regulatory costs. Industry observers expect new proposals in the next regular session of the National Assembly, which started in September.

- The legislation would put South Korea in danger of violating several provisions of their Free Trade Agreement with the United States, including KORUS Article 14.2 (Access and Use); KORUS Article 14.5 (Competitive Safeguards); and KORUS Article 15.7 (Access to and Use of the Internet for E-Commerce).

China's Extensive and Repressive Digital Authoritarianism and Protectionism

The Chinese market continues to be hostile to foreign companies, and 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 e-commerce services combined with an uptick in internet shutdowns have adversely affected foreign businesses who are increasingly hesitant to enter the Chinese market.

CCIA asks USTR to remain vigilant and discourage policies restricting foreign companies' ability to enter the Chinese technology sector, and to promote policies focused on allowing free and open competition within China's borders. This is increasingly critical as China's global dominance in technology services continues to rise.