ITI Promoting Innovation Worldwide

October 28, 2022

ITI's Comments Regarding Foreign Trade Barriers to U.S. Exports for 2023 Reporting

The Information Technology Industry Council (ITI) is pleased to respond to the Trade Policy Staff Committee's (TPSC) request for interested persons to submit comments to assist in identifying significant barriers to U.S. exports of goods and services, U.S. foreign direct investment, and the protection and enforcement of intellectual property rights for inclusion in the NTE.

The United States is a global leader in the innovation and delivery of data-driven products and services, and the U.S. economy and middle class benefit greatly from technological innovation and digital trade. As noted in a 2020 report co-authored by now-National Security Advisor Jake Sullivan, "the percentage of middle-income jobs will continue to grow in service sectors that capitalize on digital trade and other technological advances, where the United States maintains a competitive edge in the global economy."[1] Digital trade has made available immense benefits and opportunities to small and medium-sized enterprises (SMEs) – increasingly so when in-person commercial engagement is restricted – and has meaningfully leveled the playing field for enterprises of different sizes across different markets. High-tech sector workers make up a state-level average of nearly 10 percent of the total U.S. workforce, and these U.S. jobs contribute disproportionately to U.S. exports, accounting for a state-level average of nearly 30 percent of all U.S. manufacturing exports and 12 percent of all services exports.[2] Digital exports have also enabled technology companies to lead all sectors in terms of investing back in the U.S., with one report finding that technology firms are 10 of the top 25 American investors based on domestic capital expenditures.[3]

At the same time, barriers to digital trade and e-commerce have continued to emerge in markets across the world – including in the markets of some of the United States' most important trading partners – and impede U.S. exports of goods and services across a wide range of sectors. The United States' competitiveness in the digitalized global economy risks being weakened as governments pursue policies that seek to or otherwise have the effect of excluding or restricting access to U.S. information and communications technology (ICT) goods and services, or forcing value transfer from foreign to local businesses. Such trade restrictions undermine market access commitments and disproportionately hurt workers and SMEs that produce digital services or connected goods for export. Analysis by the Organisation for Economic Co-operation and Development (OECD) has shown that in relatively more restrictive services markets, new

[1] Carnegie Endowment for International Peace (2020), "Making U.S. Foreign Policy Work Better for the Middle Class": https://carnegieendowment.org/files/USFP_FinalReport_final1.pdf

[2] Information Technology Industry Council (2020), "Powering Innovation, Driving Growth: The High-Tech Economy in Communities Across America": https://www.itic.org/policy/ITI-Powering-Innovation-Report-Final.pdf

[3] Mandel, Michael and Elliot Long (2019), "Investment Heroes 2019: Boosting U.S. Growth," Progressive Policy Institute: https://www.progressivepolicy.org/wp-content/uploads/2019/12/PPI_InvestmentHeroes2019_V4.pdf

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

exporters confront costs as much as 53 percent greater than those faced by incumbent exporters.[4] As SMEs predominantly operate in the services space and frequently have limited or no export experience, countering emerging restrictions to services trade would promote the success of new and emerging firms by enabling new export opportunities.

ITI appreciates USTR's openness and responsiveness to discussions about the growing set of trade-related issues that not just the tech sector, but all sectors of the economy that leverage digital technologies and data-driven solutions, face in foreign markets. Building on notable progress in recent years, the 2022 NTE made further improvements on previous iterations in addressing many policy priorities for the tech sector, particularly forced localization policies, digital services taxes, and other restrictions to digital trade. USTR's continued efforts, in these and other areas, will continue to enable goods and services exports for U.S. companies and deepen commercial relationships with U.S. trading partners.

We are confident that the 2023 NTE will serve as an important marker in delineating our highest priority barriers to trade. However, identifying these barriers is only the first step. We also encourage USTR to prioritize work on digital issues in the following ways:

1. **Take action against digital trade restrictions that inhibit greater trade in technology products and services**. USTR's efforts to eliminate regulatory barriers and market access restrictions enable companies to participate and compete fairly in the global marketplace, which in turn promotes the virtuous cycle of private-sector research and development (R&D) investments that drive U.S. technology leadership and are made possible by sales to a diversified customer base. U.S. trade officials must therefore continue to tackle foreign trade restrictions that impact the technology sector and other sectors that use technology, and advocate for policies abroad that will benefit U.S. exports and other business activities.

   Key steps that USTR can take to achieve these goals include: (a) facilitating the flow of data across borders and promoting open internet policies; (b) prohibiting tariffs, taxes, and other barriers to cross-border data flows, digital products, digital services, and e-commerce; (c) prohibiting requirements to localize data, production, testing, infrastructure, or legal presence; (d) countering discriminatory, unilateral digital taxation measures; (e) strengthening and expanding good regulatory practices for digital trade to promote new technologies, including through risk-based governance approaches to cybersecurity; (f) ensuring that governments implement safe harbors to protect internet services from liability for activity by third parties, both with regard to copyright infringement and non-intellectual property concerns; (g) ensuring that trading partners have strong and balanced copyright rules including appropriate limitations and exceptions to drive the growth of new technologies such as machine learning; (h) prohibiting the extension of domestic telecommunications and broadcasting regulatory and licensing requirements to online services and applications; and, (i) prohibiting forced transfers and disclosure of technology,

[4] OECD (2017), Services Trade Policies and the Global Economy, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264275232-en

source code, algorithms, or proprietary information relating to cryptography. With regard to further proliferation of discriminatory, unilateral tax measures, we note in particular the October 2022 G-24 Communiqué encouraging governments to "configure a significant taxable economic presence in their jurisdictions," despite the Organisation for Economic Co-operation and Development (OECD)/G20 Inclusive Framework's efforts to finalize a Two-Pillar Approach to the tax challenges arising from the digitalization of the global economy.

In addition, we strongly encourage the continued development and strengthening of U.S. digital trade disciplines as governments enact new measures with the potential to generate barriers to trade. In digital services, for instance, governments are increasingly applying standards-based or technical regulatory governance approaches to advance policies relating to cybersecurity, artificial intelligence (AI), or industrial policy. These approaches often transpose tools traditionally used to regulate goods – such as standards-setting practices, mandatory certification, conformity assessment, labeling, or other technical requirements – to digital services. More specifically, industry has noted an increasing trend in emerging digital services policy towards reliance on country- or region-unique technical requirements or standards, the development of which lacks the transparency and due process associated with open, international standards development processes. Such technical requirements are more likely to result in regulatory divergence and incompatibility – with attendant security, trade, and economic implications.

We welcome USTR's engagement in ensuring that new regulatory approaches to digital services are undertaken in a manner no more trade restrictive than necessary to achieve legitimate regulatory objectives, and that all technical regulations – whether applicable to goods, digital services, or both – be based on global, industry-driven, voluntary consensus standards. Continuing to address these items through direct government engagement as well as through the development of new principles and rules in bilateral, plurilateral, and multilateral forums will have a large impact on the tech sector's ability to export goods and services to foreign markets, maintain the United States' status as the leading market for innovation, and increase the number of jobs created domestically.

2. **Enforce U.S. trade agreements to ensure U.S. companies and workers can compete fairly.** The rules in U.S. trade agreements should ensure that U.S. companies and workers are treated fairly and have an equal chance to compete in markets around the world. Enforcement of these rules is critical to all industries operating in the United States. We acknowledge legitimate grievances with respect to the World Trade Organization (WTO) Appellate Body, and support the goals of improving the predictability, credibility, and effectiveness of a multilateral dispute settlement system which has broadly served U.S. national and commercial interests by fostering a legal environment in which businesses can plan and grow. We therefore encourage an active and assertive approach to enforcement of U.S. trade agreements, including plurilateral and multilateral agreements to which the United States is a party, targeted at problems of significant concern.

Similarly, we support USTR's continued engagement to counter discriminatory measures that may seek to ring-fence the digital economy or otherwise target specific technology companies on the basis of subjective criteria. Particularly where they may seek to target a narrowly defined set of companies, we encourage USTR to ensure that emerging regulation is non-discriminatory and based on rigorous, objective criteria, with proportionate and well-justified obligations accompanied by appropriate due process guarantees. Such efforts build on USTR's promotion of good regulatory practices and are essential not only to avoiding potentially discriminatory impacts but ensuring that global approaches to digital and technology governance are developed in a manner that does not detract from the broader global innovation ecosystem. We appreciate opportunities to engage with USTR to discuss enforcement priorities and the available enforcement tools to address them.

3. **Actively pursue digital trade commitments with foreign governments.** The United States is a leader in the development and deployment of digital technologies that support a large and growing segment of American exports, jobs, and economic growth. The U.S. has also long been a leader in advancing ambitious international rules on digital trade. Provisions achieved in the U.S.-Mexico-Canada Agreement (USMCA) and the U.S.-Japan Digital Trade Agreement set a high standard for digital economy rules in trade agreements. In recent years, some of the United States' closest trading partners in the Indo-Pacific have sought to expand digital trade rules to serve their domestic communities and to increase their global competitiveness. For example, both the Digital Economy Agreement (DEA) between Singapore and Australia, and the Digital Economy Partnership Agreement (DEPA) among Singapore, New Zealand, and Chile, include new provisions on digital inclusion, capacity building, and SMEs. The DEA and DEPA also create formalized and regular structures for stakeholder engagement to promote the benefits of the digital economy broadly and equitably, and several governments are currently considering accession to DEPA.

   The increasing frequency of data-restrictive practices and digital protectionist measures around the world requires that the United States play a more active role in the establishment of global norms governing digital trade. Developing inclusive digital trade rules with trusted partners in the Indo-Pacific, whether through IPEF or another vehicle, should be a critical element within a broader U.S. trade agenda to counter protectionist digital economy trends, safeguard the interests of U.S. workers, and bolster U.S. political, strategic, and economic equities and opportunities in the region.

   We commend the U.S. administration for pursuing structured economic initiatives with many of the major U.S. trading partners, including but not limited to the Indo-Pacific Economic Framework for Prosperity (IPEF), Americas Partnership for Economic Prosperity, U.S.-Taiwan Initiative for 21st Century Trade, and the U.S.-Kenya Strategic Trade and Investment Partnership. As USTR and interagency colleagues identify objectives and participate in negotiations across the many engagements, ITI strongly encourages USTR to condition outcomes on a demonstrated willingness to pursue positive models for data governance and inclusive trade aligned with U.S. interests. The inclusion of binding, rules-based commitments – and the absence of broad exceptions or derogations – will complement USTR's efforts to

catalogue, address, and prevent measures that directly detract from the ability of U.S. firms large and small to engage globally.

4. **Increase efforts and resources to support a robust U.S. digital trade policy agenda.** To guide and support robust U.S. engagement on digital trade, we recommend that USTR leadership bolster resources for digital trade at all levels of the agency and leverage existing and/or new mechanisms to conduct a comprehensive review of global digital restrictions and "hot spots" of digital protectionism that negatively impact U.S. companies and workers. These steps would be commensurate with the large and growing impact of digital technologies on the global economy and U.S. competitiveness. In 2018, the Departments of State and Commerce enhanced their support for the digital economy with their digital attaché programs; we have encouraged expansion of these programs to more markets. We remain committed to working with USTR and other agencies on a whole-of-government approach that reflects the importance of digital issues in a 21st century trade policy.

We urge USTR to catalogue and take action on the foreign measures contained in this submission. These measures make it substantially more difficult for the many U.S. firms that rely on digital technologies to export their goods and services. ITI would be pleased to meet with USTR to discuss any of the content of our submission in more detail.

Contents

Argentina

Barriers to digital trade and electronic commerce

In September 2022, Argentina's Access to Public Information Agency (AAIP) launched a public consultation on a draft bill to update the personal data protection law. Although Argentina has one of the most advanced data protection regimes in Latin America, the draft bill's proposed definition of "international transfer" is overly broad, as the current definition does not acknowledge that data physically travels across borders as part of almost every online activity, even where the activity is wholly domestic and there is no change in data controller or data processor. The draft bill has several other concerning provisions, such as a 48-hour incident notification requirement for data controllers, an in-country local representation requirement for data controllers and processors, and fines based on the company's global revenue. ITI has requested that AAIP prioritize clarifying definitions and scope, including in instances where there is legitimate interest of third parties for processing data, and review the data subject's rights and duties of data controllers and processors for clarity. Doing so would help ensure appropriate compliance and avoid a burdensome regime that generates confusion for both users and the private sector and challenges the ability of U.S. companies to provide services in the market. Finally, ITI notes that AAIP initially provided an incredibly short consultation period (18 days, then extended by a few more days) that does not reflect the spirit of the Declaration on Good Regulatory Practices reached at the Ninth Summit of the Americas. While the declaration is non-binding, it underscores the importance of good regulatory practices, such as ensuring an open and inclusive public consultation that engages all interested parties in the regulatory process.

Taxation

The Argentine government (GOA) has applied a series of capital controls and new tax measures to the consumption of imports that make it more challenging for Argentine citizens to import goods and services. On October 28, 2019, the Central Bank established a limit of $200 per month that citizens were able to access through their bank accounts, limiting the amount of money those citizens could use to import goods and services. On December 23, 2019, the executive branch issued Decree 99/2019, implementing a temporary 30 percent tax ("PAIS tax") on the purchase of foreign currency and purchases made online invoiced in foreign currency, among other things. In August 2020, the Federal Administration of Public Revenue and Customs (AFIP) issued a revised opinion with the result that services rendered by non-resident entities now fall within the scope of Article 14 of the Income Tax Law (ITL), and therefore an effective withholding rate of 17.5 percent shall apply on the payments made by local customers. This new opinion stands in contrast to a previous ruling by AFIP in December 2017 and appears to contravene Article 5 of the Income Tax Law (ITL) and Article 9 of its Regulations.

Several Argentine provinces have implemented a turnover tax on the provision of digital goods and services that only applies to non-resident companies. The rates, covered activities, exemptions, thresholds, and de minimis levels all vary by province (of which there are more than 20 provincial jurisdictions that apply the turnover tax), greatly increasing the compliance burden on U.S. companies engaging with the Argentine market.

In addition, on September 16, 2020, the Central Bank introduced a 35 percent tax on foreign currency purchases, including on cross-border transactions made with credit cards, to "discourage the demand for foreign currency." Combined, these controls and taxes are making it increasingly difficult, and at times impossible, for foreign companies to sell to Argentine customers. For example, if the price of a digital service is 100 pesos, the customer pays at least 164 pesos and the service provider receives 82.5 pesos (not including transaction fees). Accounting for taxes and controls, but not accounting for inflation (36.1 percent in 2020) or the cost-of-payments, below is a reflection of what a customer in Argentina paid in 2017 versus 2021 for a company to receive the same payment:

- 2017: Customer is charged: 100 pesos | Service provider receives: 100 pesos.
- 2021: Customer is charged 199 pesos | Service provider receives: 100 pesos.

Import policies

In 2016, the GOA implemented the Comprehensive Import Monitoring System (SIMI), which established three different low-value import regimes (Postal, Express, and General). However, given the challenges that persist in clearing goods through the General import regime, only the Express Courier regime works functionally for e-commerce transactions and the limits within that regime create serious roadblocks for U.S. companies seeking to export to Argentina. The Express regime limits shipments to packages under 50 kilograms and with valuation under $1000, and imposes a limit of three of the same items per shipment. While import certificates/licenses for products are not required, the government limits the number of shipments per year per person to five, which is strictly enforced. U.S. companies have had to stop exporting to Argentina altogether given the complexities within the General regime and the inability to know how many shipments a customer has already received.

Imports to Argentina are subject to pre-shipment licenses for certain IT and telecommunication goods. There are two types of licenses: 1) Automatic license – approved within 2-3 days; and 2) Non-automatic license – approved within 7-10 days. In September 2021 GOA published a regulatory change through the AFIP and SIECyGCE (Secretary of Industry, Economy and Foreign Trade Administration) establishing an increase of response time from 10 days to 60 days, which can potentially result in delays to issuance of import licenses, delaying inbound shipment activity.

Incremental efforts to reform customs procedures and facilitate trade have unfortunately been seriously undermined by a variety of recent measures that have been adopted with minimal prior notice, consultation, or transparency. First, in March 2022, the Argentinean Central Bank issued Communication "A" 7466 through which further restricted access to foreign exchange and extended the time for approval of import licenses to up to 180 days, thus limiting the importation of all non-automatic license products. This measure was modified on multiple occasions to create special categories of products, increasing barriers to imports. Furthermore, on October 4, 2022, the Secretary of Commerce of the Ministry of Economy published Resolution 26/2022, which expanded the list of products under non-automatic license controls. This list now includes more than 4,000 HS codes, covering nearly all exports to Argentina. The Resolution entered fully into force one day after its publication, affording traders no time to adjust. A few days later, on

October 13, 2022, the Argentina Federal Administration of Public Revenue (AFIP) and the Ministry of Commerce published a regulation on the new Import System of the Argentine Republic (SIRA), which will replace the Integral Import Monitoring System (SIMI). The measure was announced with no prior notice, and came into operation on October 17, four days after its publication.

Australia

Barriers to digital trade and electronic commerce

ITI continues to track Australia's implementation of the Telecommunications and Other Legislation (Assistance and Access) Act. While Australia has gone to significant lengths to clarify the scope of the law through policy guidance published online and industry briefings, concerns remain that these areas should be clarified in the law itself. Australia is attempting to address important issues of law enforcement access to data and codify appropriate processes for requesting information from industry. It is in industry's interest that Australia employ a rule-of-law-based approach that protects industry from inadvertent exposure of customer data or creating potential network or product weaknesses. The Government appointed an independent national security advisor to assess whether the law would require revision. The independent monitor's July 2020 report found that the law had largely succeeded in protecting Australians and did not require any major revisions, but the report did present recommendations, such as the establishment of a new statutory office (the Investigatory Powers Commission) to assist in approving and issuing notices requesting access. Thus far, no amendments to the Access and Assistance Act have been introduced into Parliament per the independent monitor's recommendations.

In February 2021, the Australian government passed the Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code), after the draft bill was initially released by the Competition and Consumer Commission in August 2020. The Code requires U.S. digital platform companies that display domestic Australian news content to create a contract for revenue sharing and notify news outlets of any changes to the company's internal algorithms. While companies have not yet been designated, the Code accords the Australian Treasurer unfettered discretionary power to designate companies to which the Code should apply. As the Code would only affect U.S. companies, it appears to conflict with basic trade principles of national treatment and non-discrimination under the Australia-U.S. Free Trade Agreement (AUSFTA) and the WTO General Agreement on Trade in Services (GATS).

In November 2020, the Australian government issued the Media Reform Green Paper. The Green Paper proposes setting the "expectation" that subscription and advertising video-on-demand services invest a percentage of their Australian revenue in Australian content, in the form of commissions, co-productions, and acquisitions. If service suppliers fail to meet investment expenditure "expectations" for two consecutive years, then the Minister of Communications will have the power to implement regulatory requirements. As drafted, the proposal would not apply to Australian subscription video-on-demand service providers (SVODs) that have a free-to-air TV broadcaster within their corporate group of companies. At the same time the Australian Government established a voluntary reporting framework administered by Australian

Communications and Media Authority (ACMA) under which SVOD services report to ACMA on their level of investment in Australian content. ACMA's first report, published in August 2020, showed SVODs had invested AUD$268 million in Australian content, and the second report, covering the 2019-2020 financial year, found that SVODs spent AUD$153 on Australian programs. Were the Australian government to mandate SVODs invest a percentage of their Australian revenue in Australian content, it would *prima facie* appear to contravene Australia's national treatment commitments under the U.S.-Australia Free Trade Agreement, including specific non-conforming measures referred to in Annex II of the agreement with respect to interactive audio and/or video services.

In June 2021, Australia passed the *Online Safety Act 2021*, which came into force in January 2022. Companies have to comply with: 1) rapid content takedown powers; 2) industry codes that require companies to proactively prevent access to illegal and harmful materials; and 3) mandatory transparency reporting. Failure to comply could result in civil penalties (max. AUD$555,000 per contravention for companies), while systemic disregard for notices could result in a Federal Court order to cease providing a service in Australia. The 'Basic Online Safety Expectations' created under the Act will require international service providers to report on the steps they take to, among other things: 1) provide Australian-specific safety information from the regulator; 2) take steps to identify people behind anonymous accounts; and 3) monitor encrypted communications for harmful content. The eSafety Commissioner has also made clear that the enforceable industry codes required under the Act, which will apply to all international services accessible by Australians, need to include obligations for companies to *prevent* harm from occurring, and also to conduct regular mandatory transparency reporting. Implementation of these obligations poses technical challenges and privacy concerns, in addition to a significant regulatory burden.

In 2021, the Australian government launched a process to amend the *Security of Critical Infrastructure (CI) Bill of 2018* through the *Security Legislation Amendment (CI Bill) of 2020.* The proposed legislation significantly expanded 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, as well as enhanced cybersecurity obligations. In September 2021, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) issued an Advisory Report recommending Parliament split the draft Bill into two separate bills, including a fast-tracked version that includes mandatory oral cyber incident reporting within 12 hours and 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. Parliament accepted the PJCIS's recommendation to split the bill in two, passing the *Security Legislation Amendment (Critical Infrastructure) Act 2021* in December 2021 and the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* in March 2022.

Taxation

The Australian Treasury released in August 2022 a consultation document titled "Government election commitments: Multinational tax integrity and enhanced tax transparency," which

includes proposals that would divert from international tax norms and challenge the ability for U.S. companies to serve the Australian market. One proposal would expand the treatment of royalties to include embedded royalties, which are not generally included because they are extremely difficult to identify and value in many cases and would lead to longer and more difficult dispute resolutions. We encourage the U.S. government to underscore the importance of adopting policies that are consistent with international tax norms and Australia's treaty obligations.

Intellectual property rights

The most recent amendments to Australia's copyright safe harbor scheme, which expanded intermediary protections to some public organizations, intentionally excluded commercial service providers including online platforms. The current scheme continues to protect Australia's domestic commercial broadband providers.

Services barriers

The Australian Taxation Office (ATO) published in June 2021 a draft taxation ruling (TR 2021/D4) on royalties with respect to software payments in order "to provide updated guidance on modern forms of software distribution including digital channels and cloud computing." As drafted, TR 2021/D4 does not appropriately distinguish between payments for acquiring copyrighted articles and payments for exploiting copyright rights. More specifically for the purposes of this draft taxation ruling, the underlying rationale for classification holds true whether or not the payment arises from a software copyright holder or a distribution intermediary. A change of this nature would make Australia an outlier with respect to global norms regarding the tax treatment of payments by software resellers and distributors. This reversal of well-understood and internationally accepted guidance will not only lead to increased disputes and double taxation, but it also signals a potential forthcoming change in the tax treatment of broader intellectual property transactions in Australia with respect to resellers and distributors, such as those in digital media and streaming. While we will continue our engagement with ATO, we encourage USTR, Treasury and Internal Revenue Service (IRS) colleagues to raise concerns about the impact to U.S. companies engaging with consumers in Australia.

Bangladesh

Barriers to digital trade and electronic commerce

The Digital Security Act of 2018 criminalizes a wide range of online activity, creating challenges for internet-based platforms and digital media firms. The Act criminalizes publication of information online that hampers the nation, tarnishes the image of the state, spreads rumors, or hurts religious sentiment. The Act provides for criminal penalties up to $120,000 and up to 14 years in prison for certain infractions.

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. In November 2018 the BTRC instructed all international internet gateway licensees to temporarily block a U.S. Voice over IP service supplier; the block lasted for one day. Such interference, even on a temporary basis, undermines the value of internet-based services, decreasing the incentive to invest and raises costs for firms in the market.

Technical barriers to trade

ITI welcomes the positive updates conveyed by the U.S. Department of Commerce regarding industry's concerns about Bangladesh's Hazardous Waste (E-waste) Management Rules. When the U.S. government raised ITI's remaining concerns about the Rule at the July WTO/TBT meeting, the Bangladesh delegate indicated that the revised regulations it issued in June 2021 reflected their response to industry input and that they changed their rules to adhere to globally harmonized standards. They further indicated that the rule would not be enforced until 2026, which would give industry five years to adjust to the rule. That said, if needed, they may extend the timeframe. Furthermore, they indicated that they would hold stakeholder workshops on the rule and that they are willing to continue to discuss the issue bilaterally with the U.S. government. As background, industry first raised concerns about Bangladesh's Hazardous Waste (E-Waste) Management Rules after Bangladesh notified to the WTO TBT Committee its new rules on February 20, 2020. In response to the notification, ITI submitted comments in spring 2020 raising concerns about the need to align with globally recognized regulations such as current Restriction of Hazardous Substances (RoHS) requirements through both the U.S. and EU TBT Enquiry Points. In June 2021, Bangladesh issued a revised version of the Hazardous Waste (E-Waste) Management Rules. While the revised rule addressed many of the industry's concerns, in September 2021 ITI sent a letter to Bangladesh requesting clarifications about numerous definitions and unclear provisions in the revised rule. Industry is hoping for the identification of the point of contact to help answer industry's remaining questions regarding the rule.

Brazil

Barriers to digital trade and electronic commerce

Brazil's Institutional Security Office (GSI) has revoked Ordinance no. 9 of March 2018 and put in place Normative Instruction no. 5/2021 of August 2021, which provides for information security requirements for the use of cloud computing solutions by entities of the Federal Public Administration. There are data localization obligations for information considered classified or confidential. Additional data processed by the Federal Public Administration may be stored abroad, but only in countries previously approved by the Information Security Committee of each entity.

ITI is concerned about proposed measures that would severely impact the ability of internet and other tech companies to do business in Brazil. For example, the bill that became known as the

"Fake News Bill" (PL 2630) would put into place a set of requirements that are nearly untenable for internet companies, including onerous liability parameters and a local presence requirement. Relevant provisions would require companies to verify all accounts with a local phone number or passport, retain, trace, and monitor messages and content for three months, grant remote access to Brazilian law enforcement to any data stored outside Brazil, prevent certain messages from being shared by a given number of users, and establish high sanctions. The bill passed the Senate and was sent to the House of Representatives in July 2020, pending further consideration. ITI urges USTR to push back on the onerous elements of the Fake News Bill and to continue emphasizing that regulations must be technically feasible and find the right balance of equities in ensuring a safe, open, innovative internet economy.

The Federal Administration has embraced the goal of approving platform regulation legislation focused on content moderation, algorithms transparency, and social media. The main goal is to prevent social media platforms from removing content, even if against their terms of uses, without a judicial order. ITI is very concerned with initiatives that intend to change the internet governance model in the country, especially Marco Civil da Internet (MCI) and its liability regime.

In August 2020, bill no. 4255/2020[5] was presented to the Brazilian Senate and includes a provision requiring digital platforms to "pay news publishers for use of their content (other than hyperlinks)." This discussion has been incorporated in the debate around regulation of disinformation. Given that U.S. digital platforms services constitute a majority of digital services providers in Brazil, such a requirement stands to unfairly disadvantage and burden U.S. digital services suppliers by forcing value transfer to the publishers, while limiting the space for U.S. digital services suppliers to operate in the Brazilian market. The bill has not yet advanced in the Senate.

In 2018, Brazil adopted a General Personal Data Protection Law (LGPD), applicable both to the private and public sectors, that ITI believes strikes an appropriate balance between protecting the data subject's rights and enabling innovation and access to information. However, implementation of the LGPD has raised some concerns, notably around ensuring uninterrupted cross-border data flow of personal data. In June 2022, the Brazilian Data Protection Authority (ANPD) published a call for an initial input to discuss regulation of international data transfers, including the implementation of regulations on standard-contractual clauses and binding corporate rules (BCRS). ITI encourages Brazil to leverage global best practices in promoting clarity and predictability for companies and ensuring that business operations are not disrupted, especially where they rely on data processing and transfer outside of Brazil.

Brazil has contemplated measures to apply ill-fitting or cumbersome regulations to value added services, such as video on demand streaming or other over-the-top services (OTTs). Recent consultations by both the Brazilian Telecommunications Agency (ANATEL) and ANCINE question how to regulate these services under existing frameworks or whether to create new regulatory models, without due consideration of specific market and service characteristics, as well as the

[5] Bill no. 4255/2020 at https://www25.senado.leg.br/web/atividade/materias/-/materia/144233

technical feasibility of the requirements on these services. Specifically, ANATEL is reviewing its Competitive Market Plan and plans to include OTT as a relevant market in order to apply ex-ante regulation. ITI encourages Brazil to take an approach rooted in good regulatory practices that considers the innovative nature of internet-based business models and the overall consumer welfare, incentivizing less prescriptive regulations across all services and avoiding any potentially overly burdensome rules that would limit access to these services. ITI also encourages the permanent prohibition of customs duties for digital products and electronic transmissions to ensure that added costs do not impede the flow of music, video, software, games, or information. Additionally, ANATEL has indicated that it intends to regulate the administrative blocking of piracy content. If ANATEL decides to pursue this direction, the agency should consider safe harbors for platforms that are committed to preventing piracy in their services.

In April 2021, the Federal ICT Ministry published the Brazilian Artificial Intelligence Strategy (EBIA), which guides the actions of the Brazilian government in favor of the development of initiatives to stimulate research, innovation and development of AI solutions, as well as their responsible use. At the legislative level, some bills that intend to regulate the development and use of AI have been presented. Most recently, Bill 21/2020,[6] which includes principles for the development and use of AI, has been adopted in the House and sent to the Senate for deliberation. This bill, introduced by Congresswoman Luísa Canziani, improves significantly on earlier proposed text in its more principled and risk-based approach, and greater focus on establishing guidelines to encourage investments in R&D and create an enabling environment for new AI-based technologies. In 2022, the Senate created a special Commission of Legal Scholars to analyze the draft text of the bill and produce a report with amendment suggestions by December 7, 2022. In June 2022, the Commission held a public consultation and hosted public hearings, in one of which ITI participated as a speaker and provided recommendations. There is a growing concern that the Commission may propose provisions that would codify inflexible mandates instead of building on ongoing efforts to establish best practices in responsible AI development. ITI is monitoring this legislation and will continue to advocate for the adoption of a flexible and diversified regulatory approach that encourages strong public-private collaboration and responsible development of AI.

Moreover, in August 2022, ANPD asked for initial input to its Regulatory Agenda for 2023-2024, which included regulation of AI as a potential area of focus. Given that there are several ongoing legislative and conceptual discussions around the regulation of AI in Brazil's Congress, we have encouraged ANPD to refrain from regulating AI before the conclusion of the legislative debate to avoid creating conflicting regimes and inadvertently curtailing the development and adoption of AI technologies.

Taxation

We understand there are several proposals – both as standalone measures and as part of broader tax reform – under consideration that would seek to implement new taxes on certain digital activities. In one proposal, a "CIDE-Digital" (PL 2358/2020) would apply at a progressive rate of

[6] https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340&fichaAmigavel=nao

one to five percent (on the basis of global revenue) on revenue generated in connection with three narrowly defined sets of digital services. The Committee on Science, Technology, Communication and Informatics in the Câmara dos Deputados held a public hearing in September 2021 to discuss this legislation. Other proposals of note would establish a unique COFINS-Digital (Contribution to the Financing of Social Security) of 10.6 percent on gross revenue from specific digital services, and a 3 percent tax on gross revenue from digital services targeting the Brazilian market by companies with more than BRL 4.5 million in global revenues (PLP 131/2020 and PLP 218/2020, respectively).

Introduced by Filipe Barros (PSL/PR), the "CIDE-Internet" (PL 640/2021) would apply a 3 percent gross revenue tax on revenue "arising from the economic exploitation of the availability, distribution, dissemination or supply of content on the internet carried out in the country." Activities covered under the proposed tax include advertising, sponsorship or merchandising; content targeting; collection, distribution or processing of data; payment platform; or exploration or dissemination of image, text, video, or sound related to an individual or legal entity. Any revenue that has already been subject to taxation in Brazil would be excluded from the calculation base.

Furthermore, in the Ministry of Economy's tax reform proposal, the Ministry proposes establishing the Social Contribution on Transactions with Goods and Services (CBS), a federal contribution similar to the Value Added Tax (VAT) that could introduce significant new obligations for online service providers and marketplaces if not carefully crafted. ITI urges the Brazilian government to refrain from introducing any tax measure that is discriminatory in nature, and to recommit to finalizing a multilateral solution to tax challenges arising from the digitalization of the global economy.

Technical barriers to trade

In 2022, ANATEL took a troubling step when it introduced a draft regulation to mandate USB Type-C® mobile phone charging interfaces in the country. ANATEL based its proposal entirely on the European Union's proposal, which creates many technical barriers to trade, does not align with the European Commission's own Impact Assessment (IA) reports, and runs counter to the EU's commitments under the WTO TBT Agreement. In our comments to the WTO TBT Inquiry Point, ITI recommended that Brazil and ANATEL pursue an approach that meets the objectives for long-term environmental/consumer benefits and keeps pace with innovation while maintaining consistency with Brazil's obligations under the WTO TBT Agreement. We also requested that ANATEL closely consider the benefits of marketplace-led approaches, the unsuitability of this subject matter to regulation, the complexity and potential negative impacts of regulatory mandates, and whether policy objectives can be better met through less restrictive regulatory and non-regulatory tools.

ANATEL published Resolution no. 740/2021, which approves the Cyber Security Regulation Applied to the Telecommunications Sector and Act no. 77/2020, related to cybersecurity requirements for telecommunications equipment. Initially, those cybersecurity requirements are not mandatory for manufacturers. However, there are discussions within ANATEL to shift this

approach to mandatory cybersecurity testing requirements, which may expand to all equipment in any circumstances, including IoT devices. The Act also fails to reference international standards, which stands to cause fragmentation during implementation. ITI recommends that any regulatory schemes be technology neutral and refrain from mandating prescriptive technical features/controls as they can become outdated quickly and be at odds with the basic economics of product and services design and apply at finished product level. ITI also urges Brazil to refrain from issuing any mandatory certification requirements and to rely instead on suppliers' declarations.[7]

Regulation on Conformity Assessment and Approval of Telecommunications Products (Resolution No. 715, of October 23, 2019) prohibits the use and marketing in Brazil of non-approved telecommunications products. In 2020, Act n. 4521 (2020) was published and requires all certificated telecom products to be homologated prior to importation, except for lab testing, as of December 27, 2021. Samples for other local tests and prototypes are under specific authorizations (for Temporary Use of Spectrum or for Special Service for Scientific and Experimental Purposes). These processes are not clear and timing to grant approval is estimated from 60 to 90 days. USTR should encourage the improvement of such regulation to require only minimal information to ensure the level of confidentiality needed, especially for prototypes. In addition, to facilitate the import of products and investment in Brazil, the import process should allow entry of reasonable quantities and should be compatible with global company operations.

With respect to Internet of Things (IoT) governance, ITI recommends that Brazil support IoT security industry best practices that provide voluntary baseline capability for consumer devices, while aligning with global norms and global value chains. We further recommend looking at the NISTIR 8259 and 8259A, IoT Device Cybersecurity Capability Core Baseline. This document establishes a set of voluntary core capabilities that will help to ensure device security and is an example of a successful multi-stakeholder process in which global consensus helped to drive the outcome. In addition, we also highlight the importance of referencing international standards and encourage Brazil to participate in the ISO/IEC 27402 IoT security discussion that is currently in progress.

ITI has identified another opportunity for Brazil and the U.S. to work together to reduce barriers to trade between the U.S. and Brazil: establishing and implementing a new government-to-government agreement in the area of conformity assessment bodies (laboratories) and the acceptance of test results. The U.S.-Brazil 2020 Protocol on Transparency and Trade Rules incorporated several new commitments to strengthen the bilateral trade and investment relationship, and we see opportunity for a similarly ambitious outcome on this topic that can then be advanced in other markets. This is especially relevant as the U.S. pursues development of the Americas Partnership for Economic Prosperity, the Indo-Pacific Economic Framework for Prosperity, and other regional engagements, all of which should support putting in place Good

[7] ITI has further developed its positions on potential certification approaches to cybersecurity in our September 2020 document, "Policy Principles for Cybersecurity Certification," https://www.itic.org/policy/ITI_PolicyPrinciplesforCybersecurityCertification_Final.pdf

Regulatory Practices, deterring protectionist policies, and upholding core WTO tenets. We encourage USTR to consider how a U.S.-Brazil agreement on conformity assessment and acceptance of test results can serve as an example for other trading partners in the Americas, and globally, to transform their regulatory systems. Such a new agreement represents an opportunity to go beyond the work of previous negotiations to achieve greater levels of alignment and cooperation between our two countries and secure real benefits for manufacturing companies.

Import policies

Brazil's *de minimis* threshold of USD $50 remains applicable only to Consumer to Consumer (C2C) transactions sent through Post and does not apply for Business to Consumer (B2C) or Business to Business (B2B) transactions. There is some legal disagreement in the way that the rule is being interpreted; there exists some case law stating that the exemption should apply for both B2C and C2C transactions, and that the *de minimis* threshold should be raised to USD $100. This varied treatment of the threshold between transactions and the low *de minimis* threshold for imported items creates unnecessary barriers to trade through increased transaction costs for Brazilian businesses, and acts to restrict consumer choice and competition in the Brazilian market. ITI requests that the U.S. Government address this barrier to trade in the 2023 NTE and work with the Brazilian government to extend the application of the *de minimis* threshold to both B2C and B2B transactions, and to increase the *de minimis* threshold to a rate more in line with international standards and consumer shopping behavior.

Brazil has advanced its trade facilitation policy by implementing the new Single Window project for imports and exports. The goal of this project is to reduce the average time of customs procedures by implementing one integrated system and cutting bureaucracy and paperwork requirements. The creation of the Product Catalog, a database of products and foreign operators, is an additional component of this proposal aimed at reducing import time and increasing the quality of the product description. ITI encourages the Brazilian government to consider e-commerce particularities within this process to guarantee a simplified process for products bought online. It is crucial that the government considers the e-commerce contributions to the corresponding public consultation and ensures that businesses have proportional time to adapt to new requirements.

Products that require import licenses under the current Brazilian licensing system face import challenges mainly related to the time it takes to issue the license. Air shipments are consolidated with thousands of other products that may not require an import license, but as the license requirement is applied on a per-product and per-shipment basis, a product that requires licensing can interrupt the shipment and delivery of other products to consumers. Brazil should offer the possibility to issue an import license by product through a process that requires categories of information that correspond with those in the product catalog (i.e., there should not be a requirement to specify commercial data). It is also necessary to extend the validity of import licenses from six months to one year, and to allow for their application to multiple shipments with no limit of quantity (only time).

Finally, Brazil is one of the few countries in the Western Hemisphere that does not allow importation of remanufactured goods. The Ministry of Economy issued a Public Consultation (Circular Secex 45/2021) in July 2021 to collect information and investigate the potential impacts on the economy, industry, investments, employment and environment if Brazil were to allow the importation of remanufactured goods. Companies and industry associations sent contributions. While the process is still pending, USTR should encourage Brazil to allow for the import of remanufactured goods and parts, which can reduce consumer costs and company service costs of such goods, and help advance environmental goals by facilitating a more circular economy.

Services barriers

In November 2020, the Central Bank of Brazil (Bacen) launched a national real-time payment (RTP) under the brand PIX, which directly competes with private sector payment networks. At the same time, Bacen mandated – through regulation – the use and promotion of PIX among banks with over 500,000 accounts. Bacen's dual role as regulator and competitor has created a conflict of interest through a series of anti-competitive measures that favor the payment brand PIX. These measures stifle competition, innovation, and market evolution, in addition to compromising Bacen's neutrality with respect to payment regulation. Specifically, Bacen's Competitiveness and Market Structure Department (Decem) oversees not only the development of policy that applies to all payment schemes in the Brazilian market, but also the operations and regulation of PIX. We urge USTR to ensure the full participation of U.S. payments firms on a level playing field in the market and to keep encouraging BACEN's general adherence to good regulatory practices as a way to drive the emergence of new payment solutions and innovative business models.

Other barriers

The Government of Brazil maintains a variety of other localization barriers to trade in response to the weak competitiveness of its domestic tech industry. It provides tax incentives for locally sourced ICT goods and equipment (*Basic Production Process* (PPB) – Law 8387/91), and it does not recognize the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks (ANATEL's Resolution 323). ITI also encourages USTR to work with the Brazilian government to foster a manufacturing and trade environment that is globally competitive and provides a level playing field for all sectors of the industry.

Cambodia

Barriers to digital trade and electronic commerce

A sub-decree (Sub-Degree No. 23) 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. While the specifics of the implementation remain unclear (including but not limited to an effective date), there is potential that this could be abused and misused to block online content and keep out certain foreign digital services.

The Cambodian Interior Ministry has developed a draft Cybercrime bill[8] including broad provisions that mandate data localization to facilitate access by government authorities, as well as provisions that may impose liability on platforms for content uploaded by third parties. There has thus far not been any consultation with industry on the draft bill.

The Cambodian Ministry of Posts and Telecommunications has developed a draft Cybersecurity Law. The proposed law would introduce licensing requirements for a broad range of cybersecurity services to be provided in Cambodia, including a "cybersecurity consultation service." It would also require all ICT equipment to have a function to protect cybersecurity and ensure data security. These broad requirements would likely be challenging for U.S. industry to meet.

Canada

Barriers to digital trade and electronic commerce

In 2019 the Office of the Privacy Commissioner (OPC) proposed revising its policy position on transborder data flows under the Personal Information Protection and Electronic Documents Act (PIPEDA), to assert that a company that is disclosing personal information across a border, including for processing, must obtain consent. Although the OPC ultimately withdrew its proposal, it did so with the caveat that it would maintain the status quo only "until the law is changed." ITI has raised concerns that such data-restrictive measures may move forward in a broader, whole-of-government form, including through measures subject to public feedback as part of the February 2020 consultation on privacy and artificial intelligence (AI).

In June 2022, the Canadian government introduced Bill C-27, which would establish rules regarding trade and commerce in AI systems (Part 3: Artificial Intelligence and Data Act) and replace Canada's existing personal data protection regime (Part 1: Consumer Privacy Protection Act). While the Artificial Intelligence and Data Act (Part 3) generally takes a risk-based approach to managing certain harms that may stem from specific uses of AI systems, some key definitions, such as the "person responsible," are vague and need further clarification. For example, it is not clear how requirements would apply to a person that is designing, developing, or deploying an AI system, as opposed to a person that is "managing" an AI system. Other definitions, such as "high impact AI," remain undefined but will have significant implications for the scope of the legislation and the breadth of regulatory discretion available to the Minister of Innovation, Science and Industry. Additionally, regarding the data protection element of C-27, it is important that the Canadian government works to stay consistent across federal and provincial governments and with U.S. and EU policies, because a patchwork of policies will be burdensome and costly for both business and consumers.

A Canadian legal requirement to obtain consent for the processing of data outside of Canada would impede the flow of data across borders and serve as a de facto data localization

[8] https://www.voanews.com/a/east-asia-pacific_activists-cambodias-draft-cybercrime-law-imperils-free-expression-privacy/6196959.html

requirement, as obtaining consent from all Canadian customers, employees, or contractors, or customers would often not be possible. Placing such a restriction on cross-border transfers of data would also potentially contravene Canada's digital trade commitments under the USMCA.

The Province of Quebec adopted privacy legislation, known as Bill 64, in September 2021 that will only permit public and private sector entities (with limited exceptions) to transmit personal data outside of the province to jurisdictions with a level of protection equivalent to Quebec's privacy law. In September 2022, the first tranche of requirements came into force, including to delegate privacy officers, and mandatory data breach reporting. Other aspects of the law will gradually come into force over the next two years. Amendments to the Bill include changing the "equivalency" requirement, as it related to cross border data transfers, to an "adequacy" requirement, which has yet to be defined.

The Province of Ontario has proposed a provincial privacy law, and British Columbia is reviewing its current privacy framework. Other provinces are in the early stages of these efforts. There is a concern that restrictions on data transfers, especially if introduced at provincial level before a new common federal position is enacted, could create excessive compliance costs for businesses operating in Canada and risks to data security.

Introduced in February 2022, the *Online Streaming Act* (C-11) would amend the Broadcasting Act to encompass online undertakings and user generated content, direct how algorithms surface content for users, and give the Canadian Radio-television and Telecommunications Committee (CRTC) broad and extraterritorial oversight of the production, discovery, and dissemination of content. C-11 passed the House of Commons in June 2022, and Senate consideration is ongoing. We appreciate USTR's efforts to express serious concerns with the bill and encourage greater engagement as Senate consideration continues.

In April 2022, Heritage Minister Pablo Rodriguez introduced C-18, titled "An Act respecting online communications platforms that make news content available to persons in Canada," and also known as the "*Online News Act*." The legislation would establish a framework through which digital news intermediary operators and news businesses would be required to enter into agreements regarding news content that publishers make available to digital news intermediaries, including links and short extracts. The CRTC would administer key elements such as whether a platform meets the criteria and to help oversee mandatory negotiations, but the bill does not provide guardrails or thresholds to govern CRTC's actions. As drafted, the legislation is inconsistent with Canada's commitments under the USMCA, including but not limited to the targeting of only U.S.-headquartered companies and employing performance requirements (Article 14.10), and commitments under the Berne Convention. Canada's Parliamentary Budget Office recently estimated that $329.2 million would be paid to Canadian industry annually by just two U.S. companies. The nature of the mandatory arbitration mechanism also raises concerns about due process and transparency.

Taxation

Previewed in late 2020 and tabled in April 2021, Canada's Budget 2021 includes a DST that would

be effective as of January 1, 2022. Finance Canada then released for public comment draft legislative proposals for the *Digital Services Tax Act* in February 2022. The DST would be a three percent tax on revenues derived from online marketplace services, social media services, online advertising services, and the sale of user data, with applicability determined by a global revenue threshold of EUR 750M and an in-scope revenue threshold of CAD 20M in any calendar year. Registration for the DST would begin at CAD 10M in Canadian in-scope revenue threshold. The tax would apply to in-scope revenue above a $20,000,000 deduction. ITI submitted responses in February 2022 and June 2021 to Finance Canada consultations that encouraged Canada to continue directing its efforts to the OECD/G20 Inclusive Framework's multilateral negotiations and to refrain from advancing a unilateral DST measure. Further, the USMCA reduced trade barriers by facilitating cross-border data flows that allow companies of all sizes and in all industries to access digital services at affordable prices. The adoption of a DST would subject many of the companies delivering those essential services to tax treatment that contravenes longstanding international tax and trade norms.

Despite 137 governments (including Canada) committing to not impose newly enacted DSTs on any company until the earlier of December 31, 2023, or the coming into effect of a Multilateral Convention for Pillar One, the Canadian government on October 8, 2021 reiterated its intent to adopt a DST that would retroactively apply to January 1, 2022 if a Multilateral Convention is not in effect by January 1, 2024. We are very concerned that Canada's advancement of a DST will not only undermine ongoing negotiations to finalize the multilateral project but will embolden other jurisdictions to adopt their own measures in spite of the multilateral moratorium.

Chile

Technical barriers to trade

Despite Chile's historic record of business-friendly policies, recently we have observed the introduction of rules that impose, for example, local testing requirements and mandate specific and unique telecom labels and safety markings. ITI understands Chile is also planning to require additional labels related to other segments, such as environment and/or consumer labels. While presented as minor changes to ideally address social needs and provide information, the cumulative impact of additional, distinct labels contributes to a complex business environment that features barriers to entry and additional costs specific to participation in the Chilean market. ITI suggests the Chilean government pursue an open and transparent dialogue with stakeholders in order to develop policy approaches that meet the government's objectives but do not inherently serve as technical barriers to trade.

With regard to labeling, Chile already requires country-unique labels for mobile phones (Resolution Nº 1.463/2017), the emergency system (Resolution 1474/ 2016), and other areas. The government is discussing also requiring a reparability index (Bill n. 12.226-03), a durability determination (Bill n. 12.409-03), and an ecolabel (Bill n. 14.572-12), all implying further physical labeling requirements. Rather than providing information, a proliferation of labels, marks, and markings are likely to create confusion, increase costs, and increase the regulatory burden for companies. Particularly problematic are those additional requirements for certain goods, such as

ICT devices, where products and packaging are decreasing in size. Chile should both carefully assess the necessity, utility, and cumulative impact of existing and proposed labeling requirements, and consider the adoption of e-labeling options that allow for the presentation of compliance information in a manner that does not impeded trade. We request that USTR encourage careful analysis of the real and cumulative impact of labels before Chile adopts new labeling requirements. When such a label is determined to be needed, options such as e-labels and website communications should be prioritized to provide consumer information without unnecessary barriers to market entry for goods.

In December 2021, Chile approved a bill (Boletin N°12.409-03) that establishes measures aimed at encouraging the protection of consumer rights. This bill qualifies the duration of durable goods as basic commercial information, and therefore obliges suppliers of durable goods to provide information on their useful life, under foreseeable conditions of use. In September 2022, the Servicio Nacional del Consumidor (SERNAC), the consumer protection authority, published a resolution (N° 0773) determining how suppliers must comply with the requirements to label products with durability information under foreseeable conditions of use and period, to which the supplier is obliged to have spare parts and technical service repair. The resolution is unclear and raise questions on planned obsolescence. These implementing guidelines create Chile-specific regulations that will be burdensome and difficult to comply with as they would be country-specific. ITI urges USTR to encourage the Chilean government and SERNAC to consult with industry and collaborate with USTR to understand the trade impacts should this bill be passed into law.

ITI has seen some draft legislation introduced in Chile that would impose a common charger requirement for mobile phones in the country. ITI urges USTR to remind Chile of its obligations under the WTO TBT Agreement and encourage Chile to avoid any measures that would impose technical barriers to trade in the ICT industry.

Introduced in September 2021, Bill N°14.561-19 (also known as the Digital Platform Regulation Bill) has several concerning provisions that stand to stifle U.S. innovation and impact freedom of speech. The current definition of digital platforms in the Bill is expansive and captures virtually any entity engaged in business online or facilitating an online common interaction space for people to execute various tasks. Additionally, the Bill presents concerns around the restriction of the movement of data, as it would mandate express user consent as a necessary means for any storage, processing, or transfer of data, establishing a constructive or default localization requirement. This would set a worrisome precedent for harmful data localization and create tension with existing Chilean data protection law and international data transfer mechanisms. ITI respectfully urges the Chilean Senate to pursue a new approach to the governance of digital platforms in a manner that prioritizes transparency, coordination with overlapping and adjacent regulatory frameworks, and multi-stakeholder collaboration. ITI is monitoring this legislation and will continue to advocate for the adoption of a flexible basis for facilitating the necessary movement and processing of data available in international data protection legislation.

In December 2021, Chile published its Pro-Consumer Law n. 21.398 that includes a unique

requirement that all durable products publish their product lifespan under foreseeable conditions of use, including the period in which supplier will provide spare parts and technical services for repair. This requirement creates significant burdens and regulatory uncertainty, given that there are no clear or agreed national or international methodologies or criteria for these factors. On September 5, 2022, the Chilean Consumer Service (SERNAC) published Exempt Resolution 733 as an interpretation of the supplier's requirements to inform consumers of durability of goods. The resolution failed to provide further clarification on these requirements, but instead provided a loose definition of durability and vague guidelines on how to determine durability and "foreseeable conditions of use." These requirements create both risks and further uncertainty for businesses, including potential for fines and penalties, as well as confusion for consumers.

Services barriers

Chile is also pursuing data residency requirements for financial services. Under Chile's Comision para los Mercados Financieros, its compilation of updated rules (Recopilacion Actualizada de Normas Bancos or "RAN") Chapter 20-7 requires that "significant" or "strategic" outsourcing data be held in Chile. The same requirement is outlined in Circular No. 2, which addresses non-banking payment cards issuers and operators. In effect, these regulations can apply to any confidential records. In the case of the international movement of such data, transfer may occur, but duplicate copies of such records must be held in Chile.

China

The inability of foreign companies to obtain licenses to operate cloud services in China without a Chinese partner, data localization requirements, and ambiguous security review regime requirements remain key concerns for ITI members. These and other market access restrictions, particularly those unjustifiably portrayed as necessary for security reasons, create an uneven playing field in favor of Chinese domestic firms. We request that the U.S. government continue to highlight these problems in the 2023 NTE and re-engage with the Chinese government to address concerns.

Barriers to digital trade and electronic commerce

Data localization measures remain in China, with the previous draft implementation regulations under the Cybersecurity Law, Data Security, and Personal Information Protection Law now finalized and in force. Though there have been signs of the government seeking to identify areas for increased openness through "pilot" foreign trade zones (FTZs), particularly in Hainan, which are geared towards loosening data restrictions, the Hainan FTZ guidelines released in 2021 offered no concrete steps towards openness in the data or cloud services markets. Onerous regulations on U.S. cloud service providers (CSPs), which are at the forefront of the movement to cloud in virtually every other country, continue to effectively bar them from operating without a Chinese partner or using their brand name.[9]

[9] China's Ministry of Industry and Information Technology (MIIT) proposed two draft notices – Regulating Business

More specifically, these measures (1) prohibit licensing foreign CSPs for operations; (2) actively restrict direct foreign equity participation of foreign CSPs in Chinese companies; (3) prohibit foreign CSPs from signing contracts directly with Chinese customers; (4) prohibit foreign CSPs from independently using their brands and logos to market their services; (5) prohibit foreign CSPs from contracting with Chinese telecommunication carriers for Internet connectivity; (6) restrict foreign CSPs from broadcasting IP addresses within China; (7) prohibit foreign CSPs from providing customer support to Chinese customers; and (8) require any cooperation between foreign CSPs and Chinese companies be disclosed in detail to regulators. These measures are fundamentally protectionist and anti-competitive. Chinese CSPs remain free to operate and compete in the U.S. market, and U.S. CSPs should benefit from the same opportunity in China.

Looking beyond cloud services, data restrictions have arisen following the enactment of the Data Security Law (DSL) and Personal Information Protection Law (PIPL) in 2021, which provides three mechanisms to send personal information offshore outside of China: security certification, standard contract clause (SCC), and the Cyberspace Administration of China's (CAC) security assessment. The most tangible restrictions are found in the 2022 Security Assessment *Measures for Cross-Border Data Transfer.* While the measures were revised to distinguish between "personal" and "important" data and allow for greater reliance on self-assessments, arbitrary triggers for security assessments remain; for example, the measures are triggered by transfers of data on 100,000 or more persons abroad or transfers of sensitive personal data of 10,000 people. The passage of the DSL and PIPL in 2021 also have expanded data localization requirements, including through requirements that controllers of large-scale personal data (undefined) or CII operators store personal data within China. According to Article 42, the state cybersecurity department may also place offending organizations on a blacklist, resulting in restrictions on receiving personal information for blacklisted entities. The PIPL does not provide clarity on what constitutes a violation of Chinese citizens' personal information rights or what qualifies as harming China's national security or public interest. The trend of other nations' mirroring of these policies – particularly without any sense of how to implement them in a significantly smaller and less influential market – remains problematic. Implementation and enforcement of such policies that, for example, mandate building data centers within the country's borders, is not realistic, especially in smaller markets. This leaves the door open for uneven enforcement targeting foreign companies. Finally, the CSL creates a legal framework that institutes multiple and overlapping security review regimes for foreign technology with limited transparency and significant ambiguity that can easily preference domestic industry. The security review regimes under the CSL and related measures remain vague. These review regimes may compel companies to disclose sensitive information and create an environment conducive to uneven enforcement. The latest regulations under CSL and related laws also require services previously accessible in China from overseas websites and portals to be subject to requirements of security assessment and localization within China. This has a direct impact on U.S. companies operating within China

Operation in Cloud Services Market (2016) and Cleaning up and Regulating the Internet Access Service Market (2017). Relevant existing licensing and foreign direct investment restrictions on foreign CSPs operating in China include the Classification Catalogue of Telecommunications Services (2015) and the Cybersecurity Law (2016).

that rely on globally accessible cloud services for business operations.

On July 7, 2022, CAC officially released the *Measures on Data Exit Security Assessment* ("Measures"), which entered into effect on September 1, 2022, with a grace period of 6 months. The Measures stipulate the requirements for cross-border transfer of important data and personal information by CII operators and other companies that reach certain thresholds of data. The Measures put forward specific requirements for data exit security assessment, stipulating that data processors shall conduct a data exit risk self-assessment and specify key assessment matters before declaring data exit security assessment. In addition to the general data regulations, we have also seen data localization and cross-border data flow restrictions in various industry regulations, such as financial services, automotive, ride hailing, internet publication, mapping, and pharmaceutical sectors.

Technical barriers to trade

Though China has made positive changes in both domestic and international standards development work, problems with Chinese national standards and leveling the playing field for foreign companies' contributions remain. For example, in 2018, China finalized its Encryption Law, which requires adoption of "China-unique" encryption standards for products and services within China that do not align with the Common Criteria or other international standards.[10] The Law imposes an intrusive licensing scheme covering the sale, use, and import or export of commercial cryptography that poses significant risks of disclosure for companies. The *Commercial Encryption Administrative Regulations* also imposes a "mass market test" that would unnecessarily regulate any products that have encryption features.

While China's standardization system has become slightly more open and streamlined, China-unique standards continue to be a problem. For example, China's cryptographic standards require that information systems deployed in China use cryptographic technologies based on Chinese algorithms to protect their own security. However, these standards were originally developed by a Chinese cryptographic industrial standardization organization which does not allow foreign companies to participate.

Procurement

As a general matter, China continues to encourage that government procurements favor domestic IT companies, either explicitly with targets or implicitly through standards, local content, or other requirements that are not transparent. China's *Government Procurement Law* (GPL) was implemented in 2002 and revised in 2014. It stipulates that government procurement should purchase domestic products, services, and engineering projects, with exceptions made only when the targeted products are not available in the Chinese market or are not used within China's territory. At the end of 2020, an amendment draft calling for opinions did not result in any changes.

[10] Common Criteria is the technical basis for the Common Criteria Recognition Arrangement (CCRA), an internationally employed technical certification and mutual recognition agreement for secure IT products.

It is noteworthy that in the draft for public opinion of the *Implementing Regulations of Government Procurement Law* in 2010, the term "domestic products" was clearly defined as goods physically manufactured in Chinese territory, with a certain proportion of domestic production costs, while "domestic services and engineering projects" were defined as being supplied by Chinese nationals, legal persons, or organizations. Nevertheless, these definitions were nowhere to be found in the formal *Implementing Regulations of GPL* released in 2015. This retraction put the government procurement of foreign-invested and domestically manufactured or assembled products at a competitive disadvantage, while the government can make decisions at will if the conditions are met to be considered "domestic."

On September 1, 2021, the Critical Information Infrastructure (CII) Security Protection Regulation came into effect. This regulation boosts the procurement of "secure and trustworthy" network products and services, which results in unequal treatment between Chinese companies' products and foreign companies' products. If a company identified as a CII operator, other obligations under Chinese security legislation, such as mandatory certification and assessment and cybersecurity review, also apply, which creates compliance cost and presents a potential barrier to entry in certain sectors. Additionally, some key items (e.g., scope and obligation) lack explicit definitions.

Intellectual property rights

USTR efforts in recent years have led to some progress with respect to the protection of intellectual property rights (IPR) in China. Among significant remaining challenges to IPR protection in China is insufficient efforts by the government to guard against cross-border counterfeit crimes. In particular, industry notes concerns with (1) a lack of border measures to prevent the cross-border movement of counterfeit goods, especially as concerns sharing necessary data on counterfeits stopped at the border with rights owners; and (2) the fact that extraterritorial evidence cannot be used as formal evidence in court. The Chinese government should proactively enhance international cooperation on IPR protection, fully utilize the multilateral or bilateral mechanisms to strengthen cross-border judicial assistance, and work closely with the judicial agencies of key trading partners, including the U.S., to counter online crime.

Services barriers

When China joined the WTO in 2001, it committed to allow non-Chinese electronic payment service (EPS) companies to compete and do business in its domestic market on equal terms with Chinese companies, including by processing renminbi-denominated transactions in China. While U.S. EPS suppliers have continued to process "cross-border" transactions in China for decades, which primarily involve purchases by individuals traveling to and from China and take place in a currency other than renminbi (RMB), through the end of 2019 no U.S. EPS supplier was processing, or even authorized to process, RMB-denominated transactions in China.

Under the Phase One agreement, China committed, among other obligations, that it would accept, and make a determination on, any application for a Bank Card Clearing Institution (BCCI)

license from a U.S. EPS supplier, within prescribed time limits and without regard for the applicant's ownership structure. Following the signing of the agreement in January 2020, one U.S. EPS supplier has completed its licensing process while others have applications still under consideration. ITI welcomes steps taken by China towards fulfillment of its commitments under the Phase One agreement and the WTO Agreement and encourages USTR to hold China accountable to these commitments until all U.S. EPS suppliers that have applied for a BCCI license are able to process RMB denominated transactions, as contemplated under those agreements.

China has implemented a licensing system for telecommunications business operations. Only companies established in China, after obtaining a telecom business license, can engage in telecom business activities. Foreign companies' participation in value added telecommunication (VAT) sector is highly restrictive. Based on *Telecommunications Regulations of the People's Republic of China*, *Classification Catalogue of Telecommunications Services*, and *Special Administrative Measures for Foreign Investment Access (Negative List) (2021 Version),* foreign companies are still denied access to the business sectors critical to cloud services, namely B11 internet data center business and B12 content distribution network service.

While foreign service suppliers can earn a licensing or revenue-sharing fee through a contractual partnership with the Chinese company, the existing laws and regulations would (1) prohibit licensing foreign CSPs for operations; (2) actively restrict direct foreign equity participation of foreign CSPs in Chinese companies; (3) prohibit foreign CSPs from signing contracts directly with Chinese customers; (4) prohibit foreign CSPs from independently using their brands and logos to market their services; (5) prohibit foreign CSPs owning and operating its own data centers; (6) prohibit foreign CSPs from contracting with Chinese telecommunication carriers for internet connectivity; (7) restrict foreign CSPs from broadcasting IP addresses within China; (8) prohibit foreign CSPs from providing customer support to Chinese customers; and (9) require any cooperation between foreign CSPs and Chinese companies be disclosed in detail to regulators.

On December 31, 2020, the National Development and Reform Commission and the Ministry of Commerce released the Special Administrative Measures for Foreign Investment Access to Hainan Free Trade Port (Negative List) (2020 Version), which has in fact opened up the offshore data center business. But no application has been formally submitted up to date. Over the past one year, President Xi said China will unswervingly promote a high level of opening up, and both the central government and some local governments announced plans to open up the VAT sector in pilot Free Trade Zones (FTZs) such as Beijing and Shanghai Lingang, yet the proposed market opening has been consistently delayed.

Colombia

Barriers to digital trade and electronic commerce

While Colombia has a legal regime that allows for cross-border data flows (law 1581 2012 and Circular externa SIC 02/18), on March 1, 2021, the Ministry of Defense issued regulation 413 to implement data localization requirements for the cloud services sector. This regulation runs contrary to the national digital transformation plan adopted by the national government and

does not follow the guidelines and standards issued by the Presidential Council for Economic Affairs and Digital Transformation and the ICT Ministry. These include the Cloud Computing Manual (February 2021) and the Cloud Computing Guide G.ST.02. (May 2018), which provide definitions and scope of cloud services, and do not include data localization requirements. Similarly, the regulation is not in line with Presidential Directive 03 of 2021, which defined the guidelines for the use of cloud services, artificial intelligence, digital security, and data management in public entities of the executive branch.

Taxation

The newly elected Colombian administration introduced in August 2022 a broad tax reform proposal that included several proposals of concern, such as the introduction of a new tax on gross income derived by overseas providers of goods and digital services into Colombia. As of October 2022, the Colombian legislative bodies are considering a revised text of the bill (Article 48; formerly Article 57) that would bifurcate the gross taxation of goods and digital services from abroad. For the marketing of goods, a person becomes liable for the tax if there is a deliberate and systematic interaction with the Colombian market and obtains gross income of 31,300 UVT (approx. USD 300,000) or more in one year from users in Colombia. A deliberate and systematic interaction with the Colombian market is defined as maintaining a marketing interaction with 300,000 or more users or customers located in Colombian market during the previous or current taxable year, or providing the possibility of viewing or allowing payment in Colombian pesos. There is no threshold before the new tax starts applying for the provision of digital services from abroad. Although the drafting of the relevant provision is unclear, it appears that all gross income derived from the sale of goods and/or the provision of digital services from abroad, sold, or provided to users in Colombia, will be subject to a tax equivalent to 5%; while the revised text refers to the tax as an "income" tax, it would be a tax on gross income.

Both the original and revised texts present significant challenges to international tax norms and would create barriers to trade to U.S. companies engaging with the Colombian market. The international tax system bases taxing rights around the concept of permanent establishment (where a company has physical operations, workforce, etc.) as means of protecting against double taxation. However, a tax on gross income would mean that U.S. companies engaging with the Colombian market may be subject to double or multiple taxation on the same transaction, in addition to incurring significant compliance costs.

The Colombian government's introduction of a SEP measure, and the revised text's introduction of a gross income tax on digital services, is especially concerning given the Colombian government's participation in the OECD/G20 Inclusive Framework and its support for the October 2021 Statement that commits governments to a moratorium on the imposition of similar relevant measures and the future withdrawal of relevant similar measures for all companies.

Article 61 of the revised text introduces a new 10% withholding tax on the total payment for the sale of goods and/or provision of services made by non-residents with a SEP in Colombia.

Technical barriers to trade

Colombia is currently formulating a national AI strategy that could contain divergent standards or onerous certification or localization requirements. ITI encourages Colombia to build its AI strategy based on the facilitation of public data sharing and a flexible regulatory approach which encourages strong collaboration between the public and private sectors. Further, to promote innovation, ITI encourages the advancement of structured and standardized AI R&D, and support for STEM-informed workforce development.

Import policies

The tax reform proposal also includes a provision (Article 73; formerly Article 66) that would change the Value-Added Tax (VAT) exemption for the United States from "origin of the shipment" to "origin of the products." This would effectively limit application of Colombia's USD 200 de minimis threshold to U.S. originating goods, and exclude from scope products that are shipped from the U.S to Colombia but are not U.S. origin. U.S. shippers would also be subject to the burden of proving origin for a low-value shipment. The impact of this change would disproportionately fall on U.S. small and medium-sized enterprises (SMEs) that rely on the current Colombian de minimis threshold to reach Colombian customers. Such an approach would conflict with the U.S.-Colombia Trade Promotion Agreement's (USCTPA) de minimis commitments (Article 5.7(g)), which do not have an origin requirement for benefitting from de minimis Further, the USCTPA's chapter on Customs Administration and Trade Facilitation (Chapter 5) does not have an introductory provision that limits the scope of application of the Chapter, nor is there a provision in Chapter 1: Initial Provisions and General Definitions that would limit the scope of application of Chapter 5 to originating goods.

In December 2012, a tax reform partially implemented the VAT benefit, and on September 8, 2021, the Colombian Congress approved a new tax reform that adjusted the application of the *de minimis*. The VAT exemption for shipments under $200 will limit the application to Free Trade Agreement partners that explicitly include such VAT exemption (e.g., USCTPA) and for shipments with no commercial use. We are currently monitoring to understand how the government defines "shipments with no commercial use," and are concerned that this will impact the ability to leverage this shipment method and compliance with the USCPTA.

Services barriers

The National Development Plan Law (Law 1955) passed in 2019 included a provision (Article 154) that forces video-on-demand (VoD) providers to create a local content prominence section in their menus. This obligation was further implemented through Decree 681 of 2021 that includes a broad definition of audiovisual content and VoD services and forces providers of streaming services to identify if the user is accessing the services from Colombia.

Other barriers

While the Government of Colombia imposes certain minimum procedural requirements for the rulemaking of regulatory commissions, such as the Communications Regulatory Commission, agencies responsible for the enforcement of regulations, such as the Superintendency of Industry and Commerce (SIC), are not subject to the same requirements. This frequently leads to poorly informed, opaque, and unpredictable regulations. As one example, in November 2019, SIC

(acting in its capacity as consumer protection authority), issued Circular Externa No. 002 – November 2019, which required all mobile phone sellers and manufacturers to include a specific label on their packaging and in certain advertising that indicates a device's compatibility with all mobile network bands (e.g., 2G, 3G, 4G). The label is required for all phones, even those that operate across all bands. The SIC rule prescribes label specifications, including the content, colors, size, and placement of labels. Such country-unique labeling requirements act as barriers to trade (business must predict exact in-country sales volumes or will be saddled with inventory that cannot easily be deployed to other markets), while failing to provide much informational value, as consumers often do not see packaging until after purchase. In promulgating this rule, SIC conducted an exceedingly brief public consultation period and failed to present a regulatory impact analysis. A failure to conduct such impact analyses and—in some cases—to even allow public comment is not unusual among agencies such as SIC.

We understand that Article 10 of the tax reform legislation as revised in October 2022 would establish cascading thresholds for companies operating in Free Trade Zones (FTZs) that do not have an established export obligation (export performance requirement), regardless of if they are a goods or services company. Under the new proposal, in order to qualify for the more favorable 20% tax rate, companies will need to develop and provide an "internationalization and annual sales plan" that demonstrates the "sum of their net income from operations of any nature in the national customs territory and the other income obtained by the industrial user different to the development of its activity for which it was authorized, etc." must be below increasingly smaller thresholds, in order to maintain the FTZ tax rate. While service companies do not historically have minimum export commitments, the article as proposed does not include a carve-out for services industries.

The original text would have applied a 35% rate to non-compliant companies (and effectively eliminated the income tax rate reduction benefit from operating in FTZs), but the revised text provides that "industrial users that do not comply with the provisions of the first paragraph [performance requirements] of this article for three (3) consecutive years, shall lose the qualification, authorization or recognition as industrial users to develop their activity in free zones and shall lose free zone benefits."

U.S. companies obtained FTZ status and corresponding benefits based on specific investment and employment requirements to be performed, which did not include an obligation to draft an internationalization plan or meet a minimum threshold of exports. The imposition of new export performance requirements in FTZs contravenes commitments Colombia made under the WTO Agreement on Subsidies and Countervailing Measures, which prevents governments from creating performance requirements in exchange for receiving a direct tax benefit.

Ecuador

Barriers to digital trade and electronic commerce

Ecuadorian legislation establishes that public sector entities that contract software or related services must do so with providers that guarantee that the data remains in country and is located

in data centers that comply with international standards on security and protection. Moreover, all data related to national security and strategic sectors (the Ecuadorian Constitution defines a list of strategic sectors: energy in all its forms, telecommunications, non-renewable natural resources, transportation and refining of hydrocarbons, biodiversity, and genetic heritage, the radioelectric spectrum and water) should be located in computer centers in Ecuadorian territory. The law stipulates that data of relevance to the state that is not related to national security or strategic sectors should preferably be found in computer centers located in Ecuadorian territory or in countries with data protection standards equal to or more demanding than those established in Ecuador.

Egypt

Import policies

Effective late 2021, Presidential Decree No. 558/2021 increased tariffs on several imported products, including mobile phones, in contravention of Egypt's existing commitments through the WTO Information Technology Agreement (ITA). Notably, in addition to the 10% duty, Egypt also imposes a variety of other fees on imported mobile phones: 14% VAT, 5% "development fees," 5% airport fees, and 5% regulator (NTRA) fees. However much the above measures already impeded sales of imported phones, Egypt went a step further in March 2022 and effectively barred the importation of mobile phones altogether by requiring prior Central Bank approval to import 13 products into Egypt, including mobile phones. To date, such approval is not being provided so there is an effective ban on imported mobile phones since March 2022. In addition to a clear barrier to trade for U.S. companies, these actions frustrate and contradict the Egyptian government's stated digitalization goals, as mobile phones are a critical catalyst for digital transformation, and provide fodder to illicit trade in products, as this becomes the only channel through while mobile devices can be imported into the country.

European Union

In 2022, the European Union has continued pursuing an ambitious digital policy agenda, aimed at stepping up regulatory efforts on emerging technologies, data, and platforms. With these efforts, the EU has stated its intention to address perceived regulatory gaps and enhance the bloc's "technological sovereignty," geared towards boosting the capacity of Europe's domestic technology industry. Several recently proposed policies stand to affect the conditions under which global firms can compete in the European single market, and in some instances may entail significant extraterritorial implications.

Barriers to digital trade and electronic commerce

As part of its technological sovereignty agenda, the European Commission proposed in 2021 the first horizontal legislation for Artificial Intelligence (AI), and it is now looking to revamp its rules on data sharing. In parallel, previous legislative proposals have been finalized and adopted. These include the bloc's new rules for online platforms in the Digital Services Act (DSA), the new Digital Markets Act (DMA), which sets out to address the challenges posed by "gatekeepers," and new

rules for re-use of sensitive data held by the tech sector in the Data Governance Act (DGA).

ITI is closely involved in these legislative procedures and continues to underscore the need for the EU to pursue its policy objectives in a manner that eschews protectionism and discrimination.

Over the course of the last year, we have seen a number of policy manifestations intended in part to contribute to the European Union's vision of technological sovereignty, which remains a vague concept. Relevant policy processes currently in motion include but are not limited to:

- The two landmark proposals on platforms regulation – the **Digital Services Act** (DSA) and **Digital Markets Act** (DMA) – were finalized in 2022. The **Digital Services Act** (DSA) is aimed at harmonizing rules for the removal of illegal content online and rules related to the responsibility and liability of online platforms. It proposes new harmonized rules for flagging and taking down illegal content online, a verification mechanism for traders on online platforms, and the regulation of trusted flaggers (i.e., certified entities tasked with removing illegal content from platforms). The DSA also proposes differentiated obligations for what it identifies as very large online platforms, such as annual audits, data sharing with authorities and researchers, transparency of recommending systems, and risk management. The **Digital Markets Act** (DMA) is a law that targets large online platforms determined by Commission parameters to have a systemic role in the market. The DMA introduces obligations and prohibitions for companies that are designated as "gatekeepers" based on quantitative indicators related to revenue, number of users, and cross-border reach (across a minimum of three EU Member States). While the proposals are now finalized, ITI is continuing to follow developments as they move to the implementation phase. It remains to be seen which companies will be designated as "gatekeepers" under the DMA and what compliance with the requirements will look like for different companies. ITI encourages USTR and the U.S. administration to engage with the EU to ensure that the rules are targeted to proven and clear market failures and remain non-discriminatory in nature.
- The **Artificial Intelligence (AI) Act** was published in April 2021 and primarily targets uses of AI that the draft legislation deems to be high-risk, in addition to banning certain uses of AI such as social scoring or technologies meant to "manipulate" persons' behavior. The Commission identifies as high-risk applications including biometric identification, credit scoring, management of critical infrastructure, access to education, recruitment, and law enforcement. These AI applications would have to comply with extensive requirements related to data governance, human oversight, transparency, recordkeeping, robustness, accuracy, and security. High-risk AI systems would also have to undergo conformity assessment before being placed in the EU market. In keeping with the EU's New Legislative Framework (NLF), testing results from third-country testing bodies may be admissible only in instances in which a government-to-government agreement between the EU and a third country exists. Particularly in an area in which the application of conformity assessment is without precedent, ITI has called for more clarity and broader recognition of testing results from outside the EU to avoid creating bottlenecks in the EU testing infrastructure. Similarly, while the AI Act will presumably call for the creation of

European harmonized standards as a means of demonstrating compliance with corresponding requirements, the proposal would also allow for the Commission to develop technical specifications in the absence of appropriate standards. In this regard, ITI has urged the EU to rely on global, industry-driven standards as the means of demonstrating conformity with the requirements of the AI Act, emphasizing that doing so will help avoid global regulatory fragmentation. The AI Act is now being discussed in parallel by the European Parliament and the Council of the EU, and will most likely be finalized in 2023. ITI is advocating for a targeted definition of high-risk AI, a definition of AI that is based on global definitions (such as that developed by the OECD), proportionate and context-specific obligations and reliance on international standards. While the two initiatives are separate, we welcome the ongoing work under the EU-U.S. Trade and Technology Council to align approaches to AI under Working Group 1, as such cooperation can support facilitating regulatory compatibility.

- The **European Data Strategy** contemplates several legislative initiatives that will affect all players in the tech industry as well as other industrial sectors through increased data sharing provisions. The first legislative proposal following the European Data Strategy was the **Data Governance Act** (DGA), which was finalized in 2022 and introduces rules for the re-use of sensitive data held by the public sector. Another follow-up to the European Data Strategy is the **Data Act**. The proposal was published in December 2021, and it addresses a perceived power imbalance in the data economy by introducing an obligation for manufacturers of connected products to ensure their users can access and use the data they generate. Upon user request, this access right is extended to third parties, so long as they are not a gatekeeper by the meaning of the DMA. There would be no cost for the user for exercising this right, while access by third parties is subject to certain conditions. ITI has shared concerns on how these provisions may affect protection of trade secrets and IP, as well as on the discriminatory nature of the exclusion of DMA gatekeepers. The proposal also obliges cloud providers and other data processing service providers to remove obstacles to terminating the contractual arrangement of the service, concluding an agreement with another provider and porting the data and lays out a timeline for phasing out switching charges for customers. Cloud contracts will have to be terminated within 30 days if a customer requests so, and incumbent providers will have the obligation to port all assets to the new environment while maintaining service provision across the switching process. ITI has shared concerns on the significant burden for cloud providers as well as the impact of these provisions on cloud contracts in Europe. On international transfers of non-personal data, the proposal states that cloud providers (data processing services providers) should take “all reasonable technical, legal and organizational measures, including contractual arrangements” in order to prevent international transfers or governmental access to non-personal data that are in conflict with EU or Member states law. This raises the question of what these measures could look like in practice, and whether compliance with these requirements could effectively signify a restriction of non-personal data flows.
- Implementation of the **Cybersecurity Act**, which established a framework for the creation of cybersecurity certification schemes for different products, services, and processes with cybersecurity risk profiles. These schemes are voluntary but could become *de facto*

mandatory if, for example, individual Member States require the certificates for the provision of certain services or participation in public tenders. Work to develop the first certification schemes is under way and industry has conveyed initial concerns through multiple channels that the development and application of new certification requirements lack transparency and would create technical barriers to trade as well as barriers to services trade. This is particularly the case with the EU Cybersecurity Certification Scheme for Cloud Services (EUCS) currently being developed by the European Union Agency for Cybersecurity (ENISA), which is explored in more detail below.

- In a February 2022 Commission Staff Working Document, the EU identified "cloud and edge computing" as a strategic dependency for Europe, noting that "the EU cloud market is led by a few large cloud providers headquartered outside the EU." The EU's 2019 Cybersecurity Act established the legal basis for EU-wide certification of cloud providers. The EU agency for cybersecurity (ENISA) is currently developing a **European Cybersecurity Certification Scheme for Cloud Services** (EUCS) for adoption in 2022. In a June 2022 proposal, ENISA sought to add four new criteria for companies to qualify as eligible to offer 'high' level services, including immunity from foreign law. If adopted as written, only companies with their head office and global headquarters in an EU member state would be eligible to achieve the cybersecurity certification under EUCS. EUCS certification is a prerequisite to compete in cloud contract tenders with European governments and critical infrastructure operators; thus, the inclusion of ownership restrictions would effectively prohibit U.S. companies from competing for cloud government contract tenders for cloud projects across Europe. Provisions that discriminate on the basis of ownership violate the EU's trade obligations under the World Trade Organization (WTO) Agreement on Government Procurement (GPA) and the General Agreement on Trade in Services (GATS).
- The establishment of a unified European cloud and data ecosystem (**Gaia-X**) and European cloud federation. Gaia-X has been characterised by participants and stakeholders as a potential clearinghouse for standards, technical specifications, codes of conduct, and certification regimes developed by other organisations, which may then serve as the basis for identifying approved cloud service providers or otherwise informing European procurement specifications as well as other potential requirements. While the association is open to all stakeholders, GAIA-X recently published criteria for a three-tier cloud service labelling scheme. To achieve the highest labelling level, the "European Control" section includes requirements stating that cloud providers must: (1) be headquartered in the European Union; (2) not controlled by shareholders whose establishment is outside of the EU; and (3) adhere to limitations in the use of non-EU headquartered subcontractors. These criteria are discriminatory against companies not established under EU laws and are inconsistent with EU principles regarding freedom to provide services. Furthermore, some standards experts have noted concerns with Gaia-X governance processes and transparency, particularly as concerns the participation of non-EU entity representatives.
- The potential introduction of a new EU-wide **digital levy**. While there continues to be significant progress in ongoing negotiations in the Organisation for Economic Co-operation and Development (OECD)/G20 Inclusive Framework, the Commission has

maintained the option of introducing an EU-wide digital levy. Members of European Parliament also voted to pass a budget that includes revenue from a digital tax starting in 2023. While we understand the Commission will not be introducing a proposal imminently, we remain deeply concerned with the prospect of an EU-wide tax proposal that would attempt to ring-fence the digital economy and the enactment of unilateral, **digital services taxes** (DSTs) by Austria, France, Italy, Poland, and Spain, as well as the introduction of DST measures by four other individual EU Member States. We appreciate USTR's efforts that led to the January 2021 publication of the Section 301 Reports on Austria's DST, Italy's DST, and Spain's DST. While USTR terminated in March 2021 the Section 301 investigations into the EU's digital levy and Czech Republic's proposed DST on the grounds that the governments had not adopted the respective measures, we recognize and appreciate the clear stipulation that one or more of the investigations may be reinitiated if circumstances change. Notwithstanding the October 21, 2021 transitional agreement on DSTs between the U.S. and Austria, France, Italy, Spain, and the UK, as long as DST measures remain in place, we strongly encourage USTR to continue to use the 2023 NTE to raise the significant trade-related concerns posed by all unilateral digital services taxation measures and similar measures, including those adopted or under consideration to date in Austria, Belgium, Croatia, the Czech Republic, the EU, France, Hungary, Italy, Latvia Poland, Portugal, Romania, Slovenia, and Spain.

- The proposed regulation on distortive **foreign subsidies** that would establish new powers for the European Commission to investigate and sanction foreign subsidies determined to have distortive effects on the EU's Single Market. First explored in a June 2020 White Paper and then introduced in May 2021 as a proposal for regulation, the provisional political agreement reached in June 2022 adopts a broad, indiscriminate approach that could undermine legitimate commercial activity that benefits the EU economy and consumers. The legal instrument as proposed would establish notification-based tools to evaluate the role of foreign subsidies in concentrations (mergers and acquisitions) and procurement bids, as well as an *ex officio* general market investigation tool to examine other market situations. If, as a result of an investigation, the EU determines that an incentive that a company receives distorts the internal market, the Commission may assess corrective measures on the beneficiary to rectify the distortion, including fines up to 10 percent of global turnover, reduction of capacity or market presence, divestment of certain assets, publication of R&D results, repayment of the foreign subsidy (including an appropriate interest rate), requiring the undertakings concerned to adapt their governance structure, and acquisition denial. The proposal also generates concerns around extraterritorial impact and the potential for retaliation where governments feel measures may be unfairly targeted. Further, ITI is concerned that the EU's unilateral approach may preempt more collective action arising from, for instance U.S.-EU-Japan trilateral conversations on industrial subsidies. We are also concerned about the implications of and the proposal's deviation from the WTO Agreement on Subsidies and Countervailing Measures and other agreements. We encourage USTR to include in the 2023 NTE concerns about the structure, breadth, and administration of the proposed rule as well as unintended consequences that could arise from the proposal as provisionally agreed.

- **European Retail Payment Strategy:** The European Commission and the European Central Bank are driving a European payment sovereignty agenda that is geared at making instant payments the "new normal" and Europeanizing the payment value chain in Europe. This has been most evidenced by their support and push for the European Payment Initiative, which notably excludes non-European players from participating. The European Commission published its proposal for instant payments regulation in October 2022 and is expected to publish in Q2 2023 its proposal for the review of the Payments services directive (PSD2) together with a proposal on open finance to develop fairer access and use of data in the EU Digital Single Market.
- **European Secure Connectivity Programme**: In February 2022, the Commission released a proposal to "establish a sovereign secure space-based connectivity system for the provision of satellite services" from 2023-2027. Annex A.19 of the draft regulations, which are currently in the Preliminary Market Consultation stage, would exclude participation by U.S. companies as contractors or subcontractors to the secure connectivity programme. The European Council adopted a mandate in June 2022 to engage in negotiations with the European Parliament, which are ongoing.
- ITI understands the Commission is examining possible measures requiring payments from online service providers to broadband network providers as a mechanism for funding infrastructure deployment. The complexity of the policy landscape and of the relationships between providers of online services, including platforms, content delivery networks, and broadband network operators demands careful discussion on how to ensure competition, broader business, and consumer choice, while avoiding internet fragmentation or more broadly disadvantaging companies that operate globally. The Commission's announcement of a future consultation is a welcome and critical opportunity to engage in an open dialogue with stakeholders, particularly before any proposal is formally introduced.

Industry will continue to actively engage in the development of these policies with a view to mitigating the introduction of discriminatory and/or trade-restrictive measures, including subjective or non-proportionate scoping, possible data localization requirements, mandatory, localized *ex ante* testing requirements for certain applications of AI and cybersecurity, and closed processes for the development of *de facto* mandatory technical specifications. The ideas underpinning technological sovereignty can and should be implemented in ways that are compatible with Europe's longstanding commitments to free trade and open markets and thereby foster competitive, vibrant, and innovative digital ecosystems. They should not be based on the false premise that excluding or otherwise treating foreign entities differently is the way to strengthen Europe's technological autonomy.

Beyond potentially limiting market access, any policy approaches that serve to inhibit the movement of data as well as access to ICT goods and services may prompt other governments to follow suit, causing fragmentation of the digitalized economy. Europe should deepen its international engagement to contribute to shaping international norms together with the U.S. and its other partners to advance non-discriminatory trade and the free and open internet. This includes working together to write global digital trade rules at the WTO that advance this vision.

To that end, we applaud the establishment of the Trade and Technology Council between the United States and the EU to allow for engagement on digital trade matters of interest to either side, including open, trade-facilitative approaches to data governance and the regulation of new technologies.

The U.S.-EU Privacy Shield mechanism, which took effect on August 1, 2016, was invalidated by a landmark Court of Justice of the European Union (CJEU) "Schrems II" ruling in July 2020. At the same time, the ruling upheld Standard Contractual Clauses (SCCs) as a valid transfer mechanism under the General Data Protection Regulation (GDPR). However, it asked national Data Protection Authorities (DPAs) to scrutinize SCCs and block data transfers where protection of European citizens' data abroad cannot be guaranteed. Several DPAs have launched such investigations, the results of which could significantly disrupt international data flows.

Released on September 4, 2020, the European Data Protection Board's (EDPB) final version of Recommendations on Supplementary Measures created legal uncertainty for data transfers in the aftermath of the CJEU Schrems II judgment. Although ITI welcomes the EDPB's adoption of a risk-based approach to align with the SCCs and the emphasis on documented "practical experience" for data transfer assessments and considerations, the EDPB still maintains the two scenarios (use cases 6 and 7) where effective data transfer measures are not identified for cross-border transfers through cloud or remote access.

ITI welcomes the October 2022 signing of the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities which, along with Department of Justice Regulations, directs the steps for the U.S. to implement its commitments under the EU-U.S. Data Privacy Framework (EU-U.S. DPF). The EU now needs to approve this framework through its forthcoming data adequacy assessment. Once approved, this would provide much needed certainty for transatlantic data flows; however, we will need to remain live to the risk of future CJEU legal challenges.

Technical barriers to trade

In addition to horizontal policy efforts, the European Commission has also proposed regulating aspects of new technologies through revisions to existing vertical legislation. The EU is leading several discussions on how to regulate new technologies in parallel, including the review exercise of the Product Liability Directive (PLD), as well as sector-specific initiatives including the revision of the Machinery Directive (MD) and updates to the Radio Equipment Directive (RED). The EU's 2021 General Product Safety Regulation (GPSR) proposal further follows recently adopted legislation including the Goods Package, and specifically Regulation (EU) 2019/1020 on market surveillance of products and the Cybersecurity Act. Moreover, the update to the GPSD comes amid ongoing legislative processes around the introduction of a dedicated legislative framework through the AI Act and the recently finalized DSA. The Commission published in September 2022 a revision of EU Liability Rules in the PLD, as well as a proposal harmonizing Member States' rules on non-contractual tort-based liability rules as they apply to AI.

Each of these legislative proceedings bears significant implications for the manner in which technology firms across a wide spectrum of business models market safe and effective products and services in the EU. We strongly urge the Commission to adopt a consistent approach to the regulation of emerging technology, and one that is rooted not in regional standards but in a broad range of global, industry-driven, voluntary-consensus standards. Ensuring coherence and structured regulatory consistency across these different legislative initiatives is critical to ensure that the EU economy continues to thrive. This approach will help avoid conflicting legal requirements further down the road, while addressing proven regulatory gaps and prevent the inadvertent development of any technical barriers to trade. As indicated in correspondence with the Commission and various consultation responses, ITI believes that current laws are in most cases still fit to govern new technologies and that any legislative intervention should be based on clearly identified legislative gaps. More broadly, we are concerned that the vertical regulation of emerging technology coupled with emerging horizontal regulatory approaches risks creating legislative inconsistencies and unnecessarily restrictive requirements.

With respect to the Commission's proposed updates to the Machinery Directive, ITI believes that the Low Voltage Directive (LVD), EMC Directive (EMCD), and Radio Equipment Directive (RED) sufficiently regulate information technology equipment (ITE) and information and communications technology (ICT) equipment. Adding ITE and ICT to the scope of the Machinery Directive would only create overlapping, and perhaps diverging, requirements. If there is evidence of specific legal gaps that justifies new rules for ITE and ICT, under any directive these new rules need to be strictly targeted and should avoid legal uncertainty.

A separate Commission initiative is an amendment to the Radio Equipment Directive (RED) (Directive 2014/53/EU) to mandate a common charger for mobile devices, tablets, and other electronic devices. In response to the Commission's public consultation (in 2021) and subsequent notification to the WTO TBT Inquiry Point (in 2022), ITI strongly urged avoidance of any regulatory approach mandating the uptake of a prescriptive common charger solution and enumerated several technical barriers to trade raised by the initiative. Specifically, the EU proposal runs counter to the following: a requirement that technical regulations not be more trade-restrictive than necessary to achieve such objectives; a requirement to remove technical regulations if such objectives can be addressed in a less trade-restrictive manner; an obligation to use international standards as the basis for regulation wherever possible; and an obligation to specify technical regulations with product performance-based requirements rather than design-prescriptive regulatory measures wherever possible. We ask USTR to continue to emphasize to the EU that they should avoid technical barriers to trade when implementing regulatory initiatives.

As concerns more systemic challenges to ICT regulatory compliance, we also wish to flag issues related to the European standardisation strategy (ESS)[11] and the New Legislative Framework (NLF). Regulation (EU) No 1025/2012 provides the current legislative foundation for the NLF and,

[11] An EU Strategy on Standardisation - Setting global standards in support of a resilient, green and digital EU single market, 2.2.2022. Available at DocsRoom - European Commission (europa.eu)

alongside corresponding conformity assessment[12] and accreditation[13] legislation, establishes the legal parameters through which the Commission accords a presumption of conformity to harmonized European standards (hENs). Such standards are developed by the European Standardisation Organisations (ESOs; *i.e.*, CEN, CENELEC, and ETSI) at the request of the European Commission, or otherwise at the international level in the International Organisation for Standardisation (ISO), International Electrotechnical Commission (IEC), and/or the ISO/IEC Joint Technical Committee 1 (ISO/IEC JTC 1), leveraging legal arrangements that exist between ISO and CEN and IEC and CENELEC, respectively.

However, in recent years, we are noticing a disconcerting trendline in EU policy, whereby the European Commission has increasingly promoted policies and legislation linking European Regulatory requirements and the development of European technical specifications (e.g., Common Specifications, Codes-of-Conduct, etc.) that exclude or limit participation of non-European headquartered stakeholders in the European standardization processes. The Commission also has chosen to initiate a regional standards-dependent regulatory approach in areas where international standardization efforts are already in early stages, such as Artificial Intelligence (AI), that increases the likelihood of duplicative or non-globally harmonized standardization efforts. This trend further reflects increased intervention by EU officials in the standardization process to co-opt technical standards development in support of political objectives, including through the establishment of exclusionary, EU-unique technical specification development processes for standards intended to be adopted as regulatory requirements.

While we understand this recommendation stems from an interest in ensuring compliance certainty in the absence of harmonised European standards, industry is deeply concerned that a trend toward reliance on common specifications rather than standards will create unnecessary market fragmentation, in addition to empowering third countries to adopt similarly restrictive policies. This kind of siloed approach to standardisation in support of regulatory compliance forms the basis for a global race to the bottom, where European companies will be required to develop costly nation-specific modifications to their products in order to be able to access foreign markets. It also relocates the development of standards from expert bodies – ESOs – to the Commission itself, with the likely result that quality and market relevance of the standards produced will decline.

Additionally, the EU has undertaken a number of initiatives aiming to exclude non-EU experts from development of standards and other technical policies. Notable examples are the proposed Amendment of EU Regulation 1025/2012, which will require that only EU national standardization bodies (NSBs) can participate in the decision-making process at each stage of the development of a standard requested by the Commission, and the new rules for the selection of members of the Expert Group on Radio Equipment (RED Group), which prevent individuals from non-EU headquartered stakeholders from participating, as well as the rules for the newly

[12] Decision No 768/2008/EC
[13] Regulation (EC) No 765/2008

established High-Level Forum which allow for restricting participation from non-EU stakeholders in sub-groups dealing with critical or sensitive subjects. Taken together, these policies create potential technical barriers to trade; increase the likelihood of product and service interoperability issues globally, including security-related concerns; and set an unfortunate precedent for other countries and regions by deviating from reliance on global standards developed under an open standardization process (with participation based on equal, fair and due-process-based principles) to support technical policy objectives.

ITI continues to note that regulatory reliance on regional standards or a limited subset of international standards in the context of European technology policy may lead to unnecessary and avoidable regulatory divergence and market fragmentation in the form of new non-tariff barriers to trade and economic costs to businesses, workers, and consumers. The ICT products space is instructive in this regard: over 80 countries have technical regulations for safety, electromagnetic interference, and telecommunications; many base requirements on national standards that deviate from global norms. Particularly as the EU and other governments seek to apply standards-intensive regulatory mechanisms to digital services, there is a growing potential for global regulatory fragmentation that would have a significant, detrimental impact on trade in and access to digital services, and also limit the ability of European companies, particularly start-ups and small and medium-sized enterprises, to compete in markets outside the EU.

Moreover, to the extent forthcoming procurement, certification, and/or conformity assessment requirements for digital services are not grounded in international standards, there is a risk not only of market fragmentation (i.e., divergent requirements between jurisdictions), but of technical disruption (i.e., impact on the ability of firms to deliver optimal and secure products and services). We therefore urge the European Commission to avoid wherever possible the development of any bespoke (and therefore region-specific) technical specifications where international standards exist and can be referenced in legislation.

ITI members have noted concerns with the established processes of Harmonised Standards (HAS) consultants. We understand the review of harmonized European standards is intended to ensure alignment with corresponding harmonised Essential Requirements; however, the increased legal scrutiny, reflected in part by the intervention of HAS consultants at late stages when significant time and resources have been expended to develop consensus, is having a detrimental impact on the ability of industry to rely on hENs to place products on the Single Market. Inconsistent implementation of these checks on standards, often in a seemingly arbitrary manner, has inadvertently slowed the process of European standards development. In certain cases, it has created inconsistencies between hENs and widely used international standards. These ongoing challenges are also causing some ISO and IEC technical committees to reconsider their decisions to jointly develop standards with the ESOs. The absence of readily available harmonised standards requires industry to rely on other means to demonstrate compliance with applicable regulatory requirements, thereby undermining the predictability afforded by the NLF and disincentivizing industry participation in the development of hENs. Manufacturers must have a high degree of certainty regarding when a standard may be implemented to meet certain regulatory requirements, especially in an international and competitive market. We therefore

encourage the European Commission to review its current policies to ensure that the review of harmonized standards by HAS consultants does not unduly delay their development and publication or create divergences with international standards that could create market access barriers.

Should the European Commission continue to rely on the HAS consultants, we have urged it to adequately resource the consultant program to ensure its effectiveness. We have also encouraged the European Commission to gather feedback from experts engaged in standards development activities where progress in delivering the final work product has been inordinately delayed due to the actions of the HAS consultants.

Companies are facing disproportionate administrative barriers originating from EU environmental legislation (e.g., the WEEE, Batteries and Packaging Directives; so-called extended producer responsibility legislation (EPR)) when moving goods across borders in the EU. EU EPR legislation obligates the "producer" to register, report, and pay for certain products or materials it ships to an EU jurisdiction. The definition of "producer" is widely understood to be the seller of record. As the relevant EU legislation takes the form of a directive, country implementation is not harmonized. For example, countries have adopted varying EPR fees for different types of products, and require registration with various compliance schemes (e.g., organizations in charge of the collection of recycling fees) at the national level, as well as filing of complex reports in thousands of different unaligned categories when selling goods to the market. As a result, a seller shipping a single item into all EU countries could be required to register, report, and pay in nearly all 27 jurisdictions, under 27 different regimes. A third-party consultant estimated a cost of approximately €5,000 per country, per seller in registration and administration fees (not including the actual EPR fees). Online marketplaces are not allowed to remit fees on behalf of their sellers unless they become an "authorized representative," which requires lengthy and costly contractual arrangements between Marketplace and seller and still requires detailed product and material level reporting. These requirements tend to be prohibitive for many small and medium-sized enterprise (SME) sellers.

Furthermore, under the current regime, sellers on online marketplaces are often faced with double payments issue where the vendor pays the relevant EPR fee in the country where it places the goods on the market originally and the sellers is then asked to pay the relevant EPR fee in the country of destination if the goods are exported to another country. Some (not all) countries allow for the reimbursement of fees; however, the documentary evidence is substantial and often discourages SMEs.

Import policies

ITI would like to voice our support for the retention of the EU Customs Barriers and Trade Facilitation language from the 2022 NTE Report in the 2023 NTE Report.

The cost of compliance with VAT requirements when selling into the EU Single Market is higher for non-EU businesses than for EU businesses and constitutes a significant non-tariff barrier. The

current EU VAT registration system is generally found to be fragmented, complex and particularly costly for SMEs. This in effect restricts access to EU trade.

Services barriers

The EU has proposed regulating how EU banks and other financial companies use cloud services. This is part of a package of measures to help digitize the financial sector and modernize the EU's rulebook for the online market. The package of measures includes initiatives to harmonize companies' online defense and regulate digital financial assets. The package also includes policy strategies on retail payments and capital markets. Notably, the proposal raises concerns about dependence on a small group of U.S. providers. The bill would create an oversight system designed to preserve the stability of the EU's financial system, along with monitoring of operational risks, which may arise as a result of the financial system's reliance on critical outsourced services.

In addition to EU-wide policies addressed above, we wish to call USTR's attention to several Member State-specific initiatives.

Czechia

The implementation of the EU Copyright Directive (EUCD) in Czech law is currently in the final stages of adoption, and includes several amendments that would disproportionately affect U.S. companies, break sharply from what other Member States have implemented, and potentially weaken the ability of companies to fight misinformation and harmful content. In particular, Amendment 1274 introduces a novel set of obligations regarding Article 15 of the EUCD. This measure would target "dominant" companies, the majority of whom are U.S.-originated, with discriminatory obligations, prohibit them from "restricting" or "adjusting" their services, empower the Ministry of Culture to determine remuneration without guardrails on amounts and methodology, and require those companies to share "all data necessary" with the Ministry of Culture without safeguards for IP and trade secrets. Moreover, this amendment imposes fines of 1% of a company's total global turnover for non-compliance. This Czech measure has progressed rapidly and has not been subject to meaningful consultation with impacted stakeholders. We urge USTR to engage with Czech counterparts on the substance and process of this measure.

Separately, Czechia has proposed a novel and concerning implementation of Article 17 of the EUCD through Article 51a. This measure would potentially grant Czech legal associations and competitors the right to request the prohibition of U.S. companies' services in the event that these services repeatedly block lawful content. Such a measure would have concerning implications in terms of the ability of U.S. companies to moderate harmful content online, and moreover is unnecessary given that the CJEU has already ruled that the design of Article 17 includes appropriate safeguards to ensure user rights of freedom of expression and information.

Finland

In a communication issued in 2018, the Finnish Ministry of Finance announced its intention to introduce a requirement for companies in the financial sector to build back-up systems in Finland

in the event of exceptional circumstances and serious disruptions. In-scope companies would be subject to precautionary measures to maintain in Finland information systems and information resources necessary for the uninterrupted operation of the financial markets. Effectively, this could represent an indirect data localization requirement, presenting a market access barrier and a risk to free market and competition in Finland for CSPs that do not have local data centers. In July 2020, the FIN-FSA requested in-scope entities to submit by December 31, 2020 an entity-specific plan on how to ensure the operability and accessibility of critical services for end customers in circumstances where foreign service provision is completely unavailable. Firms' preparedness plans were requested to inform the work of the Ministry of Finance, which aims to issue legislation in 2021. Due to extensive resistance from both the financial services industry and CSPs, the issue is currently on hold with no new legislation having been communicated by the Ministry of Finance. The issue has not, however, officially been put to the side and continues to require monitoring.

In September 2021, the Finnish Institute for Health and Welfare launched a consultation regarding additional restrictions for the processing and storage of Finnish healthcare data. According to the draft decrees issued, systems that involve the provision of health and care services, and systems that contain particularly sensitive data (i.e., patient and pharmaceutical data systems) would be subject to a localization requirement. Systems handling data that is considered necessary in abnormal situations (contingency or emergency planning) must continue to operate even when network connections are limited to Finland. The physical location limitation also covers administration, backups and other maintenance solutions. Requirements also include a restriction on governance authorities of other countries having direct or indirect access to the data. If implemented, CSPs without local data centers will not be able to access and support the majority of the healthcare sector in Finland. Industry encourages inclusion of this issue in the 2023 NTE.

France

The French cyber-security agency (ANSSI) recently updated its *SecNumCloud* security certification scheme in March 2022 that disadvantages – and effectively precludes – non-EU cloud firms from providing services to government agencies as well as 600-plus firms that operate "vital" and "essential" services. France's "Trusted Cloud Doctrine" and *SecNumCloud* require that cloud providers must be "immune to non-EU laws" and, per Article 19.6, explicitly disqualify any company that is more than 39 percent foreign owned (i.e., non-EU) from certification eligibility. As *SecNumCloud* certification is a prerequisite for cloud contract tenders with the French government, U.S. companies must partner with, and transfer technology to, a local company in order to compete for cloud business with French public sector agencies and commercial entities considered "operators of vital importance." The EU's international trade commitments under the WTO GPA and GATS include the principles of non-discrimination and national treatment in terms of the nationality of persons, products, services, or technologies. Specifically, Article 19.6 of *SecNumCloud* appears to be a clear violation of Article 4 of the WTO GPA, which stipulates that GPA signatories "shall not treat a locally established supplier less favourably than another locallyestablished supplier on the basis of degree of foreign affiliation or ownership." We respectfully request U.S. government engagement to continue to raise concerns with the Prime

Minister and the Ministry of Foreign Affairs that the *SecNumCloud* qualification may not be accessible to U.S. companies on a non-discriminatory basis, and thus prevents fair trade conditions, particularly in public tenders.

In parallel to the GAIA-X initiative, France is pursuing its own "sovereign cloud program." This program is yet to be defined in detail but will likely incorporate two key components. First, it may establish legal protection for French companies from foreign laws with extraterritorial effects (including the U.S. CLOUD Act), thereby preventing any CSP from transferring customer's data to a non-EU country. The second key element of the sovereign cloud program would be the establishment of a cloud services portfolio dedicated to sensitive data and to which access would only be granted to domestic CSPs. Coupled with complications in obtaining *SecNumCloud* certification, industry is concerned that such measures will render a significant portion of the French cloud services market inaccessible to U.S. firms. Here again we respectfully request that the U.S. government raise concerns with the Prime Minister and the Ministry of Foreign Affairs.

Italy

Italy implemented the EU Regulation on Platform to Business (P2B) by appointing the Communications Authority (Agcom) as the national agency in charge of its application and enforcement. Agcom implemented the Regulation by imposing burdensome obligations on platforms that will be subject to the Regulation in Italy in a manner that goes well beyond the scope of the P2B regulation as well as actions taken by corresponding agencies in other EU member states. Specifically, Agcom passed two resolutions that implement the Regulation by: (i) forcing entities providing intermediation services to sign-up to a national registry – which involves the payment of a yearly contribution to support Agcom's activities related to P2B (ROC resolution); and (ii) requesting that subscribed entities provide extensive disclosure of internal financial and accounting data beyond what is called for in the P2B regulation itself. Agcom is also set to approve a resolution setting the amount of the yearly contribution, which will be capped at a maximum of two percent of national turnover. The two resolutions have been challenged before Italy's Administrative Court (TAR del Lazio), and a final decision by the Administrative Court is expected by the end of 2022. This decision can be further appealed before the Council of State.

Italy is implementing the EU AVMS-D (Directive 2018/1808) through a Legislative Decree (Dlgs) which enables the Government to adopt implementing measures. The Dlgs provides for, among other things, the introduction of a mandatory investment quota in European works (a quota that includes Italian works) which until 2025 would gradually increase to 25 percent of a given company's net revenues of the previous year. If the measure is approved in the current text, in 2025 Italy would have the highest mandatory investment quota in the whole of the EU.

Spain

The Spanish government transposed Royal Decree – Law 7/2021 (Sales of Goods and Supply of Digital Content Directives) into law using an implementing act passed under an emergency procedure that lacked consultation, impact assessment, and any other stakeholder involvement. The directives were directly approved by the Council of Ministers without prior announcement

despite the implementing act's diverging significantly from the text of the directives. Apart from this approach being incompatible with the general principles of transparency and stakeholder involvement to which Member States have committed under the Better Regulation agenda, the divergence from the EU texts risks creating barriers to trade, fragmenting the Single Market, and undermining legal certainty.

While Directive (EU) 2019/771 does not impose an obligation on sellers to ensure the availability of spare parts throughout a period of time as an objective requirement for conformity, Spain's national law mandates that producers ensure the existence of (i) an adequate technical service; and (ii) spare parts for a minimum period of 10 years from the date on which the good ceases to be manufactured.

Sweden

U.S. CSPs continue to face challenges in Sweden caused by the perceived conflict between Swedish law (disclosure under the Secrecy Act) and the U.S. CLOUD Act. Since the first negative statement by the *eSam* legal expert group in late 2018, we have seen a proliferation of negative statements, guidelines, and opinion pieces based on misconceptions about the U.S. CLOUD Act, and calling into question whether it is legally permissible for Swedish public sector entities to do business with U.S. CSPs. A formal public investigation began in 2019 and will run until Q3 2021 to consider 1) the legal preconditions for outsourcing IT operations; and 2) more durable forms of coordinated state IT operations. U.S. CSPs are currently engaged with the U.S. Departments of State and Commerce to resolve the issue. USTR could also serve as an effective interlocutor in the bilateral dialogue to avert the imposition of restrictions on U.S. CSPs.

Hong Kong

Barriers to digital trade and electronic commerce

Promulgated in June 2020, the national security law 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. The upcoming cybersecurity bill to strengthen the cybersecurity of critical information infrastructure might lead to new data localization requirements, which will jeopardize the free flow of data and internet to Hong Kong's business and put U.S. companies at a competitive disadvantage vis-a-vis their Chinese and Hong Kong competitors.

The Hong Kong Law Reform Commission's Sub-committee on Cybercrime issued a consultation paper that called for amendments for computer crimes involving illegal access and illegal interception to be made summary offences, i.e., acts would be criminalized without requiring malice or proof of intent to be an element of the office, but subject to a statutory defense of reasonable excuse. The Sub-committee argued that insisting on a proof of intent to commit a specific offence would cause excessive difficulty in law enforcement. However, this change would

create uncertainties for U.S. companies operating in Hong Kong with legitimate actions that could possibly rise to the level of criminal offences, particularly cybersecurity management activities conducted by personnel – for example, activities as part of an investigation of an attack or penetration – that could be construed as illegal access or illegal interception. The reversal of the burden of proof on the defendant to prove innocence or excuse, rather than for the prosecution to demonstrate intent, would lead to companies being disincentivized from offering or using cybersecurity services in Hong Kong.

India

ITI remains concerned with India's restrictive data policies, which have and will continue to generate trade barriers for U.S. companies. We recommend that USTR continue its robust engagement on these issues, both by highlighting them in the 2023 NTE as well as through direct bilateral and multilateral engagement discussion in every available forum. India has an opportunity to showcase progress on some of its more restrictive policies when it hosts the G20 in 2023. We encourage the U.S. government to work with the Government of India (GOI) to shape policies that can truly be a global model for an open foreign investment environment.

Barriers to digital trade and electronic commerce

In December 2019, GOI submitted its long-awaited privacy legislation (the Personal Data Protection Bill (PDPB)) to Parliament. Several iterations of the draft prohibited cross-border transfers of personal information except when certain criteria are met and, even when those criteria are met, a copy of all "sensitive" and "critical" personal data would still have to be stored in India. The PDPB does not define what data will be designated as "critical," an important distinction because such a designation would prohibit cross-border transfers of that data in any circumstance. The bill also required reporting of "Non-Personal Data," which would expand the scope as well as the data protection authority's responsibility to cover personal and non-personal data. In August 2022, Parliament withdrew the bill. This was a noteworthy and welcome step, but we understand that revisions to the bill are in process and expect to see a new draft soon. As the GOI looks to protect the privacy of citizens, it should do so in the least trade-restrictive manner to fulfil that regulatory objective, and not use the measures to wall off foreign companies' access to the Indian market or otherwise limit their operating space within India.

In February 2021, MeitY released the 2021 Intermediary Guidelines and Digital Ethics Code (Guidelines), which impose significant and burdensome requirements on a wide range of internet-based service providers, particularly those that operate social media, messaging, and streaming news and entertainment services. The Guidelines were notified to the Gazette of India without public consultation and are significantly different from the version MeitY had initially released for public comment in December 2018. Many of the new requirements entered into effect immediately, while "significant social media intermediaries" (5 million or more registered users in India) were given only three months to comply with sweeping regulatory changes that in some cases require significant technical re-structuring of services. These changes include the appointment of a Chief Compliance Officer, who can be held legally liable if the intermediary fails to observe the "due diligence" requirements. In addition to concerns over the lack of

comprehensive stakeholder engagement, the Guidelines contain many troubling elements that could undermine privacy, security, and freedoms of speech and expression. There are also concerns about whether the Guidelines force the localization of company operations and restrict market access for non-Indian companies through the imposition of burdensome regulatory requirements that erode safe harbor protections in India's Information Technology (IT) Act and significantly overstep international best practices. Additionally, the Indian government is reported to currently be working on a significant revision to the IT Act governing intermediary liability protections in India (the Digital India Act).

The Telecom Regulatory Authority of India (TRAI) released recommendations on a proposed Regulatory Framework for cloud services providers (CSPs) in September 2020, including a proposal for all CSPs to register with a government-controlled trade association. While TRAI's recommendations are currently non-binding, they will be sent to the Department of Telecommunications (DoT), which will decide whether to accept them as binding and determine next steps for implementation. TRAI's recommendations include: (1) mandatory enrollment of all CSPs with a DoT-controlled industry body, failing which, telecom service providers will be disallowed from providing these CSPs with infrastructure services; (2) government oversight of the industry body, including the ability to issue directions, rules, and standards, and to cancel registrations of "errant" CSPs; and (3) an exemption for channel partners and SaaS businesses, which may voluntarily enroll in these industry bodies. These proposals create an unnecessary barrier to trade by placing restrictions on CSPs' operations. In the medium-to-long term, they also pose a risk of "nationalizing" CSPs by granting them "critical infrastructure" status.

Initially released in January 2019 for consultation, India's draft E-commerce Policy represents the GOI's official position on a host of digital economy issues. The 2019 draft was explicitly discriminatory and contemplated: (1) broad-based data localization requirements and restrictions on cross-border data flows; (2) expanded grounds for forced transfer of intellectual property and proprietary source code; (3) preferential treatment for domestic digital products and incentives for domestic data storage in India (e.g., provision of infrastructure, incentives to domestic data center operators). The policy also introduces the notion of community data as a "national resource" where countries are "custodians" over data. A revised draft of the E-Commerce Policy has been in the works since the release of the draft. Media reports have suggested that: (i) certain categories of data such as defense, medical records, biological records, cartographic data, and genome mapping data should not be transferred outside India; and (ii) certain categories of e-commerce data should be mirrored/stored in India (with the government/a proposed e-commerce regulator deciding the categories). Further, the rules would impose obligations on all e-commerce entities without regard to unique e-commerce models and inter se relationships between the entities, buyers and sellers. It is unclear how the requirement for every e-commerce entity to register itself with the DPIIT is connected with protection against unfair trade practices by e-commerce entities. It would also create an arbitrary and artificial distinction between offline sellers and e-commerce entities as registration requirements do not apply to offline sellers. Such additional non-tariff barriers have a dampening impact on the market access of foreign players into the Indian e-commerce market and significantly affect cross-border flows of data. We do not expect DPIIT to release a revised draft E-Commerce Policy

in the immediate future but will remain vigilant.

GOI's Department of Science & Technology introduced in February 2021 new guidelines relating to geospatial data and associated services. While the Guidelines for Acquiring and Producing Geospatial Data and Geospatial Data Services including Maps (Guidelines) were ostensibly aimed at opening up India's mapping policy and improving the ease of doing business through deregulation, they also contain elements that are discriminatory to foreign service providers. For instance, the Guidelines provide preferential access to Indian companies to access geospatial data and develop geospatial services in India by prohibiting foreign entities from creating and owning geospatial data finer than a certain spatial accuracy 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/data is prohibited. There is also a localization requirement for such data, which has to be stored and processed on a domestic cloud or on servers physically located in India.

On September 19, 2022, GOI released the draft India Telecommunications bill (2022), which intends to replace the existing legal framework governing telecommunication in India that has been in place for more than a century. The draft text definition of "telecommunications services" is extremely broad, including broadcasting, e-mail, voice mail, voice, video and data communication services, audiotext services, videotex services, fixed and mobile services, internet and broadband services, satellite-based communication services, internet-based communication services, in-flight and maritime connectivity services, interpersonal communication services, machine to machine communication services, and over the top (OTT) communication services. Expanding the scope of the telecommunications services to include all internet-based communications services, OTT communications services, etc., could subject these businesses to additional compliance burdens and in many cases to overlapping regulations. For example, many of these businesses are already regulated through India's IT Act. The addition of a fresh and potentially duplicative set of potential licensing licensing/registration requirements may prevent these companies from bringing world-class services to India consumers, potentially change their business models, and hamper bringing fresh investments in India. We urge USTR to highlight key concerns with the proposed Telecommunications bill to the Government of India, specifically the Department of Telecommunications.

Taxation

ITI greatly appreciates USTR's efforts that led to the January 6, 2021 release of Section 301 Report on India's Digital Services Tax and encourages USTR to prioritize engagement with GOI in support of withdrawing the Equalisation Levy (EL). However, GOI has since implemented through Finance Bill, 2021-2022 an even further expansion of the EL examined in the Section 301 Report on India's Digital Services Tax.

Whereas the April 2020 revision expanded the EL to include a two percent tax on the sale of goods and services to Indian residents by non-Indian e-commerce companies, the April 2021 expansion fundamentally expanded the scope of existing rules to bring offline transactions within scope if any one of the following transaction aspects happens online: acceptance of offer for sale;

placing the purchase order; acceptance of the purchase order; payment of consideration; or the supply of goods or provision of services, partly or wholly. Further, the entire amount of consideration received for sale of goods or provision of services is considered in scope, even when the underlying good or service is provided by an unrelated third party and the e-commerce operator's income is only a portion of the gross amount received.

The design of the EL explicitly excludes Indian companies from its scope, thereby acting as a trade barrier for U.S. e-commerce companies that are competing against both Indian e-commerce companies as well as Indian brick-and-mortar establishments. While ITI has concern with the underlying premise of the measure, the lack of sufficient guidance has continued to raise significant compliance challenges with the April 2020 and April 2021 expansions. ITI appreciates USTR's efforts to conclude its investigation of the EL and urges USTR to continue stressing to GOI that the EL further contributes to the fragmentation of the international tax system and undermines ongoing multilateral negotiations under the auspices of the Inclusive Framework.

In Finance Bill 2018-2019, GOI proposed a significant economic presence (SEP) measure but deferred implementation until 2022-23 in deference to the ongoing work in the Inclusive Framework. The SEP rules came into effect on April 1, 2022. The Department of Revenue issued a notification in May 2021 to set the SEP revenue threshold at INR 20 million (about $270,000; equal to the threshold for the Equalisation Levy). If revenue from a nonresident's activities (defined as transactions related to any goods, services, or property, and explicitly including the provision of data or software downloads in covered services) pass the threshold **and** a nonresident company is engaged in systematic and continuous business activities or interactions with at least 300,000 users, then the nonresident company is liable for income tax in India. We understand that for relationships already covered by tax treaties (e.g., the U.S.-India Income Tax Treaty that has been in effect since January 1, 1991), GOI would have to amend existing tax treaties to include the new SEP definition. However, the implementation of the SEP measure is very concerning in the context of ongoing multilateral negotiations.

Technical barriers to trade

India's Compulsory Registration Order (CRO), which requires manufacturers to submit product samples from each factory for testing by a "BIS recognized laboratory" located in India, remains a primary concern for the tech industry. Under the CRO, companies are required to retest products to meet India-specific safety requirements, despite having already passed tests in internationally accredited labs. The registration process is incredibly costly to U.S. firms, and fails to improve product safety. To compound concerns, in 2020 MeitY proposed expansion of the CRO to cover additional products and components; however, it failed to perform any risk or regulatory impact assessment to justify these additions. In fact, stakeholder meetings revealed that the emphasis now seems to be on limiting imports of products into India from third countries, rather than on product safety and risk to the Indian public. These vague aims have served as the basis for unusual government requests to companies, such as the provision of employee passports and birth certificates. The intent of these requests is unclear and only slows product certification and investment in India.

We ask that USTR emphasize the importance of regulating products based on risk rather than country of origin. ITI has also asked the GOI to consider as a standard practice setting the effective date of any CRO regulation as one year from the date on which *all* of the following are complete: product series guidelines and FAQs issued by MeitY, Test Report Format issued by BIS, BIS portal ready to accept applications, and labs accredited by BIS and ready to accept products for testing. It would also be helpful if India moves ahead with a phased implementation of CRO instead of introducing two or more phases simultaneously. We recommend that USTR continue to highlight these issues in the 2022 NTE and in direct engagement with Indian trade officials.

India's Telecommunications Engineering Centre (TEC) administers the Mandatory Testing & Certification of Telecom Equipment (MTCTE) for all telecom products regulated under India's Telegraph Rules. MTCTE mandates a wide range of technical requirements from electromagnetic compatibility (EMC) and safety to security testing and IPv6 interoperability, as well as environmental requirements, among others. We appreciate USTR's support in encouraging TEC to remove testing requirements for products that already fall under the scope of CRO (i.e., commercial off-the-shelf (COTS) servers). In May 2022, TEC officially announced exclusion of five product categories from MTCTE, because they are already tested and certified under CRO. Furthermore, in June 2022, the government extended the implementation timeline of Phases 3 and 4 under MTCTE to July 2023. However, industry continues to experience on-going challenges with in-country testing requirements. India lacks sufficient capacity and infrastructure in the country to meet the demands of in-country testing for many of the MTCTE parameters (they often accept international test reports six months at a time or refuse to accept reports from any country "that shares a land border with India"). ITI continues urging the authorities to follow global best practices and accept international test reports and certificates when applicable, to allow for additional consultation with industry, and adequate transition times. We request support from the U.S. government in this process.

In mid-2022, another issue arose based on TEC's treatment of products based on country of origin. Products in the MTCTE scope require certification before the products can legally be sold in the Indian market. Industry regularly undertakes compliance testing and certification of telecom products at TEC-accredited labs in India, according to the regulation. Meanwhile, Trusted Product Approvals under the National Security Directive on Telecommunication Sector (NSDTS) are required only for products sold to Indian telecom service providers (TSP). However, some original equipment manufacturers (OEMs) make telecom equipment that is not intended to be sold to a TSP. In mid-2022, TEC began requiring products from China to have both MTCTE and Trusted Product Approvals, regardless of whether the equipment is sold to a TSP. ITI pointed out to TEC that, given the regulatory intentions and scopes of NSDTS and MTCTE, we do not believe telecom products from a particular country should be required to get Trusted Product Approvals in order to get MTCTE certifications. ITI requested that Trusted Product Approvals be decoupled from MTCTE certification for telecom products made in China (or any particular country). ITI requests support from the U.S. government in discouraging regulation based on country of origin.

Industry is also concerned about India's "Final Draft of Chemicals (Management and Safety)

Rules." The concerns are primarily with Rule 12 (2) of the "Articles" provision. We believe that safety instructions for Articles should not require Safety Data Sheets (SDSs) for chemicals for ICT products, which are durable consumer goods designed not to release chemicals. SDSs are normally used for cataloging and identifying potential chemical hazards regarding chemical hazards in an occupational setting, whereas an SDS is not intended to be used for products designed primarily for consumer use. In addition, Chapter 4 requires that a person who has control of an Industrial activity in which a Hazardous Chemical is handled must provide evidence to the concerned authority that steps have been taking to provide people working with the equipment with adequate "training and equipment including antidotes necessary to ensure their safety." For ICT products, in normal usage, providing training and equipment including antidotes is not necessary just because chemicals are in the Article. Our members believe there are more appropriate ways – including ways that would be more understandable for consumers – to provide safety instructions through ICT Articles than through SDSs.

Regarding treatment of plastic waste, India does not have a single federal mandate; instead, each state has its own independent rules, which leads to inconsistencies and high costs for industry. Industry urges GOI to find a way to ensure consistency in its plastic waste rules across the country, and that its rules are consistent with treatment of plastic waste in other major economies. In addition, the ICT sector is awaiting India's response to a remaining question regarding India's final amendments to the draft Plastics Waste Management Rule issued in July 2022. Specifically, industry would like the Ministry of Environment, Forests and Climate Change to explain the process for producers to obtain the exemption for the use of plastic sheet below 50-micron thickness in accordance with the new amendments.

Another pressing concern for the tech sector is India's restriction on the importation of refurbished and used ICT equipment. ITI member companies' used equipment shipments are often not approved for importation by the GOI and must go through a burdensome process to be imported. The processes in place to allow importation of refurbished spare parts for the provision of warranty services is not consistently observed in all ports and is extremely cumbersome, requiring charted engineer certificates for each import and detailed tracking of products flows into/out of India. This directly impacts normal warranty and repair operations for the technology sector, which utilizes refurbished parts and international repair facilities to honor warranties for consumers, businesses, and the government. The uncertainty caused by the delays and restrictions on imports of these parts has already cost ITI companies millions of U.S. dollars and threatens to severely restrict future investments in India. ITI requests that the U.S. government include this issue in the 2023 NTE to push GOI to simplify the importation process, remove port inconsistencies, and allow the importation of legitimately repaired, refurbished, and used ICT products to satisfy warranty and service contracts.

Import policies

A continuing concern for our industry is India's breaking of its WTO tariff bindings on a growing list of ICT products that were bound to zero when India joined the Information Technology Agreement (ITA). In 2014, 2016, and 2018 India levied tariffs on several products that are bound to zero as part of its yearly budget review process. It also did so outside of the budget review

process in the summer of 2017, as part of its implementation of the new Goods and Services Tax (GST), in December of 2017, in October of 2018, and most recently in April of 2021, after India's Minister of Finance proposed further increasing tariffs on printed circuit board assemblies, camera modules, connectors, and other ICT inputs. India now imposes duties of 20 percent on telecommunications products such as switches and base stations, a 20 percent tariff on mobile phones, a 10 percent tariff on certain parts for telecommunications equipment, a 10 percent tariff on ink cartridges, and a 7.5 percent tariff on parts and accessories of test equipment. The continuous and unpredictable application of these tariffs has significantly decreased business certainty and inhibited the ability of U.S. companies to plan their business operations in India and throughout their supply chains connected to India. Furthermore, despite policy clarity on classification and duty structures across different telecommunication products, shipments have been withheld and questioned due to country-of-origin issues.

Indian officials have erroneously argued that the products for which they have raised tariffs are not covered under the ITA because technology has changed dramatically since the agreement was signed. Such arguments belie a broader and often explicit effort by the Indian government to pressure companies to localize more of the ICT supply chain in India, and constitute a unilateral and discriminatory interpretation of what goods are covered by ITA commitments. In recognition of India's violation of its multilateral commitments, the EU, Japan, and Taiwan are pursuing dispute settlement cases at the WTO. We are concerned that, if left unchallenged by the United States, this trend will undermine the integrity of tariff bindings made at the WTO by all of its participants as countries seek new tools to force local production of goods, to the detriment of U.S. companies operating in and exporting to India and around the world. This is a high priority issue for the tech sector that directly impacts the ability of American companies to export to India. Industry appreciates USTR's attention to this issue so far, and we encourage USTR to continue raising this in the 2023 NTE, and to work with partners and allies to enforce WTO commitments by holding India to its bindings on tariffs on ICT products and inputs.

Indonesia

Barriers to digital trade and electronic commerce

The Government of Indonesia has a history of forced localization measures that favor local companies at the expense of foreign competitors. The Ministry of Communication and Informatics' (KOMINFO) Regulation 82/2012 (GR82) was at the center of these concerns, although we have seen some positive progress in the revised edition of GR82 with the passage of Regulation 71/2019 (GR71). GR71 has made several improvements to previous data localization provisions contained in GR82, and we commend USTR for its extensive work on these issues. However, in the draft implementing regulations of GR71, storing and processing of data offshore by any electronic systems provider (ESP) will require prior approval from the Minister. No further clarity has been provided on the circumstances under which data can be stored and processed offshore by in-scope ESPs. Moreover, while the new regulation simplifies data categories into public and private sector data, allowing the latter to be stored off-shore, it also allows scope for financial sector authorities – including the Bank of Indonesia (BI) and the Financial Services Authority (OJK) – to further define sector-specific requirements, which creates

continued uncertainty for U.S. financial services companies operating in Indonesia.

The Indonesian government could also implement additional mandatory local content requirements through the introduction of a quota or import ban as an extension of the "Neraca Komoditas" (commodity balance) policy, which is intended to force domestic production using trade imbalance as a rationale for quotas or outright bans. ICT and electronic devices may be included in the scope of the policy, which could be introduced as an extension of the Ministry of Finance PMK Reg. 26/2022 updating the Indonesia Customs Tariff book. The import ban or quota would likely be issued by the Ministry of Trade, and then the Ministry of Industry would establish the scope of targeted products. We urge the U.S. government to advise against local content policies in its engagements with the Indonesian government.

On September 20, 2022, Indonesia passed its first comprehensive Personal Data Protection (PDP) Act, which is expected to enter into full effect by 2024. The PDP is intended to bring Indonesia's privacy laws into closer alignment with international data privacy standards; however, the PDP limits cross-border data transfers and data localization requirements to countries determined to have the same standard of data protection as Indonesia, even though there are no guidelines on assessing the data protection level across jurisdictions. We are also cautious of more restrictive data localization provisions that could be included in the implementing regulations for the PDP. For example, Article 2 of the PDP claims extraterritorial reach, which is concerning for data controllers and processors located outside Indonesia. The data transfer requirements, which were previously under GR82 and amended and superseded by GR71, could potentially be contradictory to the envisioned regime of the new PDP Act, such as the restrictions on the financial services sector. We encourage the U.S. government to continue to engage Indonesia on the implementation of the PDP law to ensure the forthcoming regulations do not create barriers to trade or discriminate against U.S. firms.

In 2018, Indonesia's Ministry of Finance (MOF) issued Regulation No.17/PMK.010/2018 (Regulation 17), which amended Indonesia's Harmonized Tariff Schedule (HTS) Chapter 99 to add: "Software and other digital products transmitted electronically." Chapter 99 effectively treats an electronic transmission as a customs "import," which triggers a number of negative implications including: 1) the imposition of customs import requirements (including declaration and other formalities) that will be impossible to meet for certain intangible products; 2) the imposition of import duties and taxes on each electronic transmission; 3) the creation of security risks; and 4) the constraint of data flows into Indonesia. The inclusion of "software and other digital products transmitted electronically" in Indonesia's HTS contravenes Indonesia's commitment under the WTO Moratorium on Customs Duties on Electronic Transmissions, a commitment that Indonesia reaffirmed as recently as June 2022. Indonesia's actions have established a dangerous precedent and will likely have the effect of encouraging other countries to violate the WTO Moratorium.

While the tariff rates remain at zero, companies have expressed concern over the potential administrative burden of this new regulation, including potential customs documentation or reporting requirements; MOF has indicated that any data reporting under this system will be

voluntary. In addition, using a tariff schedule for the application of such duties on non-physical products raises fundamental questions and challenges related to the harmonized tariff system, the role of customs authorities in the digital space, and the determination of country of origin for electronic transmissions. If implemented on a mandatory basis, these customs duties would be levied on the same electronically supplied services (ESS) that are subject to a VAT in Indonesia. The inclusion of "software and other digital products transmitted electronically" in Indonesia's HTS contravenes Indonesia's commitment under the WTO Moratorium on Customs Duties on Electronic Transmissions, a commitment that Indonesia reaffirmed as recently as June 2022. In order to eliminate this barrier, Indonesia must rescind Regulation 17 and remove Chapter 99 from its HTS. We appreciate USTR's bilateral and multilateral work to address this issue, and we strongly encourage continued engagement with the Indonesian government to resolve it.

Government Regulation no. 80 of 2019 on e-Commerce (GR80) prohibits personal data from being sent offshore unless otherwise approved by the Ministry of Trade through a list of countries which can store Indonesian e-commerce data, with little clarity on the criteria. GR80 entered into force in November 2019 without transparent opportunities for stakeholders to review and provide comments, and the regulation provided economic operators with a two-year transition period to come into compliance. The language of the regulation appears to impose burdensome licensing requirements on e-commerce operators which may restrict market access for foreign firms seeking to leverage e-commerce platforms to sell into the Indonesian market.

Trade Regulation 50/2020 on E-Commerce, an implementing regulation of GR80, also requires e-commerce providers to appoint local representatives if they have over 1,000 domestic transactions annually, promote domestic products on their platform, and share corporate statistical data with the government. Both GR80 and TR50 impose *de facto* data localization measures and local content requirements, which increase overhead costs for foreign entities and create undue market access barriers. Specifically, the regulation appears to give the Indonesian Ministry of Trade discretion in authorizing the transfer of personal information outside of the country, with little clarity on the parameters that would need to be satisfied to ensure that companies can continue to predictably move data across borders. Finally, GR80 seeks to impose an extraterritorial income tax on non-resident firms, creating the potential for both double taxation and discrimination against U.S.-based companies.

The Ministry of Communications and Information Technology (KOMINFO) has issued Regulation No.5/2020 and No.10/2021 requiring all foreign electronic system operators (ESO) serving Indonesian customers to register locally by December 2021. KOMINFO requires substantial paperwork to meet this requirement such as translation of the company's deed of establishment and legalization by the Indonesian consulate, and ESOs that are unable to register can be blocked.

Indonesia continues to contravene its WTO binding tariff commitments by charging tariffs on a range of imported technology products that are covered by Indonesia's commitments under the Information Technology Agreement (ITA) and should receive duty-free treatment. Indonesia has only implemented ITA commitments that fall under five categories of goods/HS codes

(Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods). Further, Indonesian customs has also sought to re-classify technology goods that have similar functions into dutiable HS codes that are outside of the five categories as a means to raise revenue, but in most cases the reclassified HS codes are also themselves covered by Indonesia's ITA commitments. This practice widely affects the IT industry and negatively impacts U.S. investors and their workers.

Taxation

On March 31, 2020, the Government of Indonesia adopted several digital tax measures through an emergency administrative decree (Law 02/2020). First, a corporate income tax would apply to foreign digital services companies that were determined to have "significant economic presence" (SEP). Second, an electronic transaction tax (ETT) would apply to the sale of goods and services over the internet by foreign digital services companies if a bilateral tax treaty (such as the U.S. Tax Convention with the Republic of Indonesia) prevented the application of the SEP provision. The ETT legislation provides for a measure that blatantly discriminates against foreign companies as it only applies to non-Indonesian operators. Furthermore, these digital tax measures are inconsistent with prevailing international tax principles (particularly the traditional definition of a permanent establishment) and create a significant trade barrier to U.S. and other foreign companies operating in the Indonesian market. While to the best of our knowledge the Government of Indonesia has not expressed an intent to move forward with implementing regulations for ETT, we understand the 2021 omnibus tax bill included provisions that effectively establish rules for the collection of ETT, in addition to collection of income tax, value-added tax, and other taxes. ITI strongly encourages USTR to continue its engagement with the Government of Indonesia to underscore the detrimental impact of unilateral tax measures on the global tax system and to reiterate the importance of achieving a multilateral, consensus-based solution through the OECD/G20 Inclusive Framework.

Technical barriers to trade

Local content requirements and attempts to facilitate import substitution remain pervasive issues for non-Indonesian companies, and President Jokowi has instructed the Ministry of Industry, among other agencies, to take efforts to facilitate reliance on local inputs, rather than imports. Import substitution plays a large role in President Jokowi's agenda to enhance local manufacturing across a wide range of industries, in particular for ICT products.

In 2019, KOMINFO released two regulations (No. 9 of 2019 (Wavelength Division Multiplexing) and No. 10 of 2019 (Internet Protocol Networks)), that included a requirement to "meet the Domestic Component Level in accordance with statutory provisions." No previous notice was given for the local content requirement, nor were specifics provided on the levels that must be met. In September 2020, the Indonesian Ministry of Industry released Regulation No.22/2020 (IR22) on the Calculation of Local Content Requirements (LCR) for Electronics and Telematics, with a government target to achieve 35 percent import substitution by 2025. IR22 provides specific and extensive requirements for manufacturing and development for both digital and non-digital physical products. The policy will place an additional administrative burden on the production of physical ICT products that are needed for ICT companies to operate in Indonesia.

This comes in addition to the earlier noted indications that the Indonesian government may introduce an importation threshold for ICT equipment ("Neraca Komoditas"). The government has signaled intention to build on this LCR requirement and add similar LCRs for software and applications, which would impact companies that provide services over the internet, including cloud services. Additionally, Presidential Instruction Number 2 Year 2022 requires government agencies to plan, allocate, and realize at least 40% of the national budget for goods/services to utilize MSMEs and Cooperative products from domestic production.

Under Regulation Number 159 of 2019, the Directorate General of Posts and Information Resources & Equipment (SDPPI) has been accepting international test reports on EMC, safety and telecom, without a local test and without inclusion of an Indonesia local standard in the test report. However, this has been an interim solution and SDPPI has been issuing amendments approximately every six months that extend acceptance of international test reports for six-month intervals while at the same time reducing the list of international labs from which they will accept test reports. Industry has encouraged SDPPI to continue to accept international test reports indefinitely, noting that the piecemeal changes create unpredictability that raises barriers to trade.

As a general matter, industry regularly experiences challenges with a lack of notification and compliance timeframes in burdensome regulations issued by SDPPI. Per the WTO Technical Barriers to Trade (TBT) Agreement, governments should provide at least 60 days to comment on a draft regulation or standard. Multiple SDPPI final regulations have been published without notification of draft regulation, and we have even seen cases where SDPPI has released regulations with effective dates that occur before the date of release. ITI requested from SDPPI, via letter to the Agency, at least a one-year transition time for any new regulation, a time period that is practical and achievable with reasonable assurance of uninterrupted market access of products. Finally, industry has encountered regulations or standards where the requirements are vague or unclear. Establishment of an inquiry point in SDPPI to field such questions would greatly facilitate industry compliance.

Finally, beyond those examples noted above, ITI members are seeing attempts to encourage import substitution on display through legislation such as Government Regulation 28/2021 Clause 38, which requires product certification bodies to ensure testing and certification processes are carried out by Indonesian citizens, which renders compliance processes more difficult for exporters to Indonesia.

Services barriers

In late December 2020, Bank of Indonesia (BI, the Central Bank) issued a new Payment System Regulation (BI Regulation 22/23/PBI/2020) that went into effect on July 1, 2021, and addressed several aspects of the payments ecosystem. BI also issued an implementing regulation for Payment System Providers, and Payment Infrastructure Providers in July 2021. The new regulation (PBI SP) introduces new license requirement for Payment System Providers (PJP) and Payment Infrastructure Providers (PIP), foreign ownership caps for PJP (85 percent) and PIP (20 percent), and limits on voting rights. For foreign companies who are already in the market, BI

provides an exemption through a grandfathering clause which allows foreign companies to retain their foreign ownership shares and controlling rights as long as there are no changes in share ownership after the regulation is implemented and its parent company issues a guarantee letter.

The new PJP definition includes the following activities: provision of source of fund information, payment initiation and/or acquiring services, administration of source of fund, and remittances services. The new PIP definition includes clearing and final settlement. Those international payments companies classified as PIP are undergoing conversion of their license. PJP and PIP will further be categorized into three classifications depending on their scale and possible impact on the financial system. BI may impose further requirements depending on these categorizations, which includes requirements on capital injection, risk management, and information system security. PJP and PIP will be assessed based on the size of their operations, interconnectedness, complexity, and substitutability. These categories are: Systemic Payment System Operator, Critical Payment System Operator, and General Payment System Operator.

The PBI SP requires that all domestic transactions be processed onshore end-to-end (initiation-authorization-clearing and settlement). The regulation includes a provision that allows for offshore processing subject to approval from BI. As per the National Payment Gateway (NPG) regulation (additional detail below), currently domestic debit transactions must be processed onshore and routed via the NPG. Cross-border and domestic credit transactions remain routed via international networks and processed offshore for now.

The PBI SP introduces a risk-based approach for product approvals. BI categorizes three levels of risk when assessing companies' request for approval (Low, Medium, and High): Low requires notification to BI, while Medium and High requires approval from BI. The regulation also gives authority to a local industry body to broadly determine digital payment pricing, including determining network membership fees. This provision has yet to be implemented and would be globally unprecedented. Finally, PJP and PIP are required to share data and/or information related to payment system via periodic and incidental reporting to BI. BI may also require other parties who work with PJP and PIP to share their data and/or information related to information when necessary. The regulation also outlines provisions for real-time capture of data through a data infrastructure organized by BI or integrated payments interface (yet to be developed).

In May 2019, BI released an Indonesia Payment System 2025 Vision (IPS 2025). The IPS 2025 Vision includes five key initiatives: 1) open banking and interlink between Bank-Fintech; 2) development of retail payments; 3) development of wholesale payments and financial market infrastructure; 4) creation of a data hub; and 5) regulation, supervision, licensing, and reporting. Initiative 5 covers the BI regulation on Payment Systems outlined above that was issued in December 2020 and went into effect July 1, 2021.

Over the past several years, Indonesia has adopted a series of measures that prohibit cross-border electronic payment systems and require payment processing to take place locally. These measures, including the most recent BI Regulation on Payment System 22/23/PBI/2020, BI Circular 17/52/2015, BI Regulation 18/40/2016, BI 19/8/2017, and POJK no. 38 present

substantial challenges to continued investment and innovation by U.S. electronic payment companies in Indonesia.

NPG regulation (PBI 19/8/2017), issued on July 6, 2017, established the NPG and three new institutions: a switching body, a services body, and a standards body. The NPG regulation requires any entity wishing to process domestic transactions to apply for a new NPG switching license. Criteria to obtain a new license include i) onshore processing of transactions, and ii) a cap of 20 percent on foreign ownership. Obtaining an NPG switching license would require processing of all domestic transactions according to pricing and rules as set out by a new NPG "Services Institution," comprising the domestic switches and banks and adopting standards set out by the Standards Body (this role is fulfilled by the Indonesian Payment System Association, ASPI). The new Services body, PT Penyelenggara Transaksi Elektronik Nasional (PT PTEN), is a consortium made up of the four domestic switches (Artajasa, Rintis, ALTO, Jalin) and the 4 largest banks (BCA, Mandiri, BRI and BNI).

On September 20, 2017, BI released implementing guidelines (PADG 19/10/2017) for the NPG regulation (PBI 19/8/2017) along with three appendices (including pricing guidelines which set a cap on the Merchant Discount Rate for regular domestic debit transactions of 100 bps). These guidelines establish high-level criteria for commercial partnerships between NPG and non-NPG switches, subject to approval by BI. The published criteria establish that, if a foreign payments company enters into a commercial partnership with maximum two out of four local NPG players and has on-shore processing capabilities, it would be allowed to process its own branded domestic transactions on behalf of its NPG switching partners. Two of the international networks have received approval from BI for commercial partnership with local NPG switches for domestic debit processing.

BI regulation no 21/18/PADG/2019 requires Indonesia's Standards of QR code (QRIS) for payment to be used for all QR domestic and inbound cross-border transactions. The regulation also creates categorizations for parties involved in QRIS transactions: front-end provider, NPG switches, Merchant Aggregator and National Merchant Repository, sidelining any roles of foreign principal/switching. The regulation only allows Current Account and Prepaid to be a source of funds for QRIS and requires banks to first get a recommendation from Indonesia's Payment System Association (ASPI) to add Debit and Credit cards as a first step before requesting BI approval. This creates a burdensome approval process. For in-bound cross-border transactions, the regulation only allows issuing and/or acquiring Banks in Category IV to establish a partnership to enable foreign-managed sources of funds and/or foreign-issued payment instruments.

BI still requires core/important financial transactions to be processed domestically. That said, the Financial Services Authority (OJK) has incrementally allowed some electronic processing systems to be based offshore for banking services, insurance services, multi-financing services, and lending-based technology. Despite some progress, the overall policy requires businesses to domestically process their financial transactions.

Procurement

In line with higher level concerns with local content requirements noted above, in February 2021, the Government of Indonesia issued Presidential Regulation Number 12 of 2021 concerning Government Procurement of Goods/Services (PR 12/2021), which amends Presidential Regulation Number 16 of 2018 (PR 16/2018). Under the regulation, goods and services offered for government procurement must contain a total Domestic Component Level (Tingkat Komponen Dalam Negeri – TKDN) value plus Company Benefit Weight (Bobot Manfaat Perusaaan – BMP) value of at least 40 percent. Imported products may be procured provided that: (i) the goods are unable to be produced domestically; or (ii) the domestic production volume does not meet the needs.

The regulation came into effect on the date of issue and was implemented without any opportunity for stakeholder input and lacking a notice period. To this point, we are unaware of any non-resident ICT company having been able to meet the 40 percent TKDN requirement. The regulation states further that central and regional government agencies shall procure goods and services from local micro, small and medium enterprises (MSMEs) or cooperatives. Government entities must devote at least 40 percent of their procurement budgets to buying goods and services from MSMEs or cooperatives. Bigger companies are encouraged to form partnerships with local MSMEs or cooperatives to improve their capacity.

The Government of Indonesia very publicly and at the highest levels encouraged swift implementation of the local content regulation. More broadly, the ICT sector has been specifically targeted. Building on previous statements by the President of Indonesia to implement import substitution policies, the Minister of Industry encouraged ICT products to be produced by the national industry, using TKDN requirements.

Clarification requests to the Indonesian government have been met with silence, and we ask for the U.S. Government's help in engaging with Ministry of Industry and SDPPI on these issues.

Import policies

Despite Indonesia's commitments in the WTO ITA to duty-free treatment on a wide range of ICT products, ITI's member companies have reported facing duties on certain products covered under the ITA, most recently through the MOF's PMK Reg. 26/2022 update of the Indonesia Customs Tariff Book. These products include printers and related parts, networking equipment, switches, servers and server racks, optical modules, and optical cables, as well as other ICT products. Specifically, Harmonization System (HS) Codes 84 7170 91, 84 7170 99, 85 1762 49, 85 0440 11, 84 4331 91, 84 4331 99, 84 4399 90, 84 4332 21, 85 2580 40, 85 2580 39, 85 0440 19, 85 0440 90, 85 2859 10 have inconsistently applied tariffs from Indonesia's bound-rate obligations under its WTO Goods Schedule. Indonesia has only implemented ITA commitments that fall under five categories of goods/HS codes (Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods). In addition, Indonesian customs officials have reportedly been reclassifying ICT products from codes that are duty-free in Indonesia's tariff schedule to codes that now incur customs duties, but in most cases the reclassified HS codes are also themselves covered by Indonesia's ITA commitments. These unanticipated additional costs significantly impact an importing company's

investment and operation and increase the cost of doing business in Indonesia. We strongly encourage USTR to raise this issue during engagements and request that the Government of Indonesia eliminate these duties and the trend of increasing tariffs that started in 2019 despite Indonesia's WTO ITA commitments.

Indonesia currently prohibits the import of refurbished products into the country, even when the products are supported by warranty from the product principal vendor. This presents a particular challenge for products that have reached end-of-sale and are no longer being produced as new products but maintain requirements for warranty support or replacement by users in Indonesia. For other products still in manufacturing production, refurbished products also help support the circular economy and provide more cost-effective alternatives to users in Indonesia. However, such refurbished products cannot be imported into Indonesia.

Foreign direct investment

Indonesia currently imposes restrictions on foreign direct investment (FDI) related to e-commerce. This impairs the ability of U.S. firms to invest in Indonesia and provide local e-commerce offering. Non-Indonesian firms are prevented from directly retailing many products through electronic systems and limited to 67 percent of ownership for warehousing, logistics or physical distribution services provided that each of these services is not ancillary to the main business line. Indonesia should liberalize its FDI restrictions related to e-commerce, which limit the ability of Indonesia to grow its digital economy.

Japan

Services barriers

Effective February 2021, Japan established a new regulation on "platform-to-business" (P2B) relations that requires online intermediaries to meet aggressive transparency obligations concerning differentiated treatment and access to data. These rules are targeted to "specific digital platforms" that will be assigned by the Ministry of Economy, Trade and Industry (METI) under certain thresholds. The Japanese government maintains this new law will for the time being only target App Markets and Online Shopping Malls, but METI retains authority to expand application to other types of platforms like Digital Ads and Search without changing the law.

The Japanese Ministry of Communications (MIC) recently expanded the application of its telecommunications law to foreign services. These changes are expected to oblige foreign over-the-top (OTT) services using third-party facilities (potentially including search, digital ads, and other services that intermediate two-party communications) to (1) assign a local representative to notify and register as a service provider; and (2) observe obligations under its Telecommunications Business Act (TBA).

The Japanese government launched the *Information Security Management and Assessment Program* (ISMAP) in 2020, which assesses the security of public cloud services. The requirements in ISMAP have resulted in major compliance burdens and costs to cloud service providers. For example, the ISMAP requirements go beyond relevant International Standards Organization (ISO)

standards, and compliance with international standards does not preclude companies from mandatory, costly, and burdensome audit processes. Only four audit firms are certified to conduct audits for ISMAP, resulting in long wait times and high costs for audits. Applications are also reviewed only once every quarter rather than a rolling basis. We encourage the U.S. government to emphasize with their Japanese counterparts that this approach, while intended to protect data in Japan from outside threats, denies local governments access to state-of-the-art cloud services and leaves agencies to rely on older on-premise systems and technology that are less secure.

Kenya

Barriers to digital trade and electronic commerce

Adopted in 2019, Kenya's Data Protection Act[14] provides for extra-territorial application of its requirements on data processors and controllers but does not include a clear definition of what actions bring a foreign business within its scope. Such vague and broadly scoped requirements limit certainty and present *de facto* barriers for new digital platforms and service providers entering the Kenyan market. The Act also gives the government some residual power to mandate that certain types of data shall be processed through "a server or data centre located in Kenya" and requires that the Data Commissioner be provided with proof of the security of data before it may be transferred outside of Kenya. The Data Protection (General) Regulations, 2021 require the "[processing] of personal data for the purposes of actualising a public good" to occur through a server and data centre located in Kenya, and that "at least one serving copy of the concerned personal data is stored in a data centre located in Kenya." Purposes that require such treatment are broadly scoped, such as "managing personal data to facilitate access of primary and secondary education in the country," "managing any electronic payments systems licensed under the National Payment Systems Act," and "managing any system designated as a protected computer system." Registration for data controllers and data processors opened on July 14, 2022.

Kenya's 2020 National ICT Policy Guidelines require that Kenyan data collected by the government for the purpose of providing public services "remain in Kenya."[15] Kenya's ICT Policy also includes a clause on "equity participation." The policy increased local ownership rules from 20 percent to 30 percent; companies must comply within two years for existing licenses and three years for new licenses. If these provisions are enacted, only firms with 30 percent "substantive Kenyan ownership" would be licensed to provide ICT services. This policy does not have a direct effect on the implementing bodies, namely the Kenyan Communications Authority and the Office of the Data Commissioner, but it does set a direction of travel for those agencies.

Taxation

Kenya's Finance Bill, 2020 first established a 1.5 percent tax on gross transaction value for services sold through a digital marketplace. Draft Income Tax (Digital Service Tax) Regulations, 2020 were released in July 2020, and the measure came into effect on January 2, 2021. While the

[14] http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019
[15] https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf

tax initially applied to resident and nonresident firms and could be offset by corporate income tax payments for companies with permanent establishment, subsequent legislating through Finance Bill, 2021 effectively made the DST more discriminatory against U.S. firms by excluding resident firms from scope and eliminating the ability to offset DST payments against corporate income tax payments. The legislation passed in 2021 also amended the scope to include "business carried out over the internet or an electronic network," and expanded the definition of "digital marketplace" to "an online platform which enables users to sell or provide services, goods or other property to other users." Revisions in Finance Bill, 2022 have now excluded income earned by a person with a permanent establishment in Kenya.

ITI urges USTR to encourage Kenya to refrain from collecting the DST and instead re-commit to the multilateral project through the Inclusive Framework to address tax challenges of the digitalizing global economy. This is especially important as Kenya has not lent its support to the OECD/G20 Inclusive Framework's October 8, 2021 Statement that commits participating governments to provide for the removal of relevant unilateral measures for all companies. Further, the Kenyan government's comments in response to the Inclusive Framework's latest consultation stated that "[this] provision in the Multilateral Convention would constrain the sovereignty of the domestic legislature from making future laws."[16] The Two-Pillar Solution depends in large part on the removal of relevant unilateral measures for all companies, in exchange for the establishment of new taxing rights. Maintaining a unilateral measure also presents serious implications for U.S. exporters in the form of trade barriers for in-scope companies vis-à-vis domestic competitors.

Korea

Barriers to digital trade and electronic commerce

In May 2020, the National Assembly adopted amendments to the *Telecommunications Business Act* (TBA) and the *Network Act* to require value-added telecommunications services (VATS) providers operating in Korea to appoint a local agent, take measures to ensure network quality, and potentially moderate content. In September 2020, the Ministry of Science and ICT (MSIT) and Korea Communications Commission (KCC) issued a draft Presidential Decree of implementing measures pursuant to the amendments. While these were intended to clarify the scope and requirements of the amendments, the text remains vague. It would impose burdens on large, predominantly foreign firms to take technical measures to prevent network traffic congestion, technical errors, and enable stable server capacity. Affected companies would also be required to consult with telecommunications operators on such technical methods and provide notification of unstable service. The potentially significant costs of such measures create a distinct trade barrier for U.S. companies should they be implemented as drafted. We encourage the U.S. government to work with MSIT and KCC on this issue to avoid the creation of market access barriers and avoid conflicting with U.S.-Korea Free Trade Agreement (KORUS) obligations.

[16] https://www.dropbox.com/s/kn3lj3gjd4selwo/public-comments-received-on-the-progress-report-on-amount-a-of-pillar-one.zip?dl=0&file_subpath=%2Fpublic-comments-received-on-the-progress-report-on-amount-a-of-pillar-one%2FKenya.pdf

As internet traffic increases in Korea due to increased use of applications (e.g., streaming video, video conferencing, and gaming), Korean internet service providers (ISPs) have been pressured to increase network capacity and meet a sharp increase in demand from their customers. The ISPs' solution has been to establish a "network use fee" that would allow ISPs to demand payment from a content provider for the service of delivering the content to the end user (i.e., traffic charges). However, the network use fees are redundant, as the end users have already paid ISPs for the service when they subscribe to receive internet access. Additionally, there is no evidence to support claims that ISP costs have soared as a result of the increase in internet traffic. Some National Assembly members have introduced bills that seek to indirectly impose the mandated payment by referring to "prohibited acts" stated in the TBA, including "imposing an unreasonable or discriminatory condition on the use of ISP's network to provide digital content" and "unfairly refusing to enter into an agreement or refusing to perform an agreement that has been entered into, without a justifiable reason." The introduction of these fees for content providers could distort the ISP's incentives and lead to increased traffic congestion if content providers refuse to pay the double-charge for the same service. We encourage the U.S. government to continue raising this issue with the Korean government and highlight the negative impacts such fees would have on Korean internet consumers, as well as emphasizing these policies would be counterproductive to Korea's ambitions to become a global digital hub.

In October 2020, Korean legislators in the National Assembly proposed six bills that would amend the TBA to ban app stores from requiring that app developers use a uniform billing system. On August 31, 2021, the Korean Legislative Assembly's Legislation and Judicial Committee passed the "In-App Legislation," which bans large app store operators from requiring app developers to use their respective in-app payments systems. The law appears to run contrary to Korean trade commitments by taking an approach that would disrupt standardized practices that ensure consumer privacy, security, and reliable access across markets, and with legislators' public statements effectively singling out two U.S.-headquartered companies. The law will also restrict U.S. app developers' ability to reach the Korean market via trusted ecosystems.

ITI appreciates the U.S. government's attention to the issue of spatial information and mapping data in Korea, which it has acknowledged in past reports. Article 16 of the *Spatial Information Act* continues to prohibit transferring any maps or "fundamental surveys" out of Korea without permission from the authorities. Such restrictions limit access to the Korean market by foreign suppliers and significantly impede business operations that rely on mapping or GPS data. We hope that this issue is addressed again in the 2023 NTE.

Technical barriers to trade

While Korea has been a member of the Common Criteria Recognition Arrangement (CCRA) since 2011, the National Intelligence Service (NIS) has imposed since October 2014 additional domestic cybersecurity certification requirements through its Security Evaluation Scheme (SES). The purpose of the CCRA is to ensure a globally uniform standard for product security assurance and remove the need for additional verification or certification between countries. The Korean government, however, has broadly imposed the SES for internationally CC-certified information

technology products to be sold to the public sector.

The NIS, which controls Korea's security certification system, revised the SES in early October 2022, by dividing all public institutions into three sensitivity tiers and allowing institutions in the middle and lower tiers, such as universities and public schools, to use internationally CC-certified ICT products without additional domestic security verification by the NIS. However, the SES still applies to most major public institutions that account for an overwhelming proportion of the public sector market, including all central administrative institutions such as ministries and metropolitan local governments, and continues to act as a TBT. We encourage the U.S. government to urge the Korean government to abide by obligations as a CCRA member and abolish the Korea-unique SES.

The Korean Executive Branch and the Korean National Assembly have both issued numerous proposed amendments to Korea's environmental regulations over the past year. Industry has confronted many proposed amendments to Korea's packaging, recycling, energy efficiency, and circular economy rules. Not all proposed rules are notified via the WTO, and many have tight comment periods. Industry would appreciate more time for consultations with industry and English translations if possible. Many of the rules will be difficult to implement and industry would appreciate the opportunity to provide input to help the government achieve its environmental goals in ways that are achievable for industry.

Procurement

The Korean government has instituted a number of policies under the guise of promoting small and medium-sized enterprises (SMEs) that discriminate against U.S. multinational companies. The *Act on Facilitation of Purchase of Small and Medium Enterprise-Manufactured Products and Support the Development of Their Markets* categorizes companies by size, with multinationals frequently labeled as "large" and local companies reaching the "small" or "medium" thresholds. As such, "large" foreign companies are only able to bid on (the rare) projects larger than USD $220,000, while most local companies can bid on the majority of projects available. This is particularly problematic for non-Korean companies because even if the size of their business is small, they are categorized as "large" due to their foreign ownership, and thus are deprived of opportunities to participate in various bids. Similarly, the *Software Industry Promotion Act* restricts bids for certain government contracts for software services to "small and medium-sized" entities, again, leaving multinationals out of the government procurement process. These policies are largely driven by the National Assembly and the Ministry of SMEs and Startups (MSS). In addition to posing preferential treatment problems, the policies also preclude Korean entities from choosing from a full selection of products and services, leading to higher prices and lower quality.

Significant barriers to the adoption of public cloud services still exist. In 2016, the Korea Internet and Security Agency created a Cloud Security Assurance Program (CSAP) governing public sector cloud service procurement. The CSAP is a technical barrier to trade (TBT) for U.S. cloud service providers (CSPs) in the Korean public sector market, as U.S. firms are unable to meet some components of the certification program without creating a separate Korea-unique product, like

physically segregating facilities for exclusive use for government-owned customers and the use of Korea-specific cryptographic algorithms. Such an approach undermines the economies of scale of cloud computing and thus one of its primary benefits. It also appears unprecedented among developed countries, which, apart from national security applications, have permitted a "multi-tenant" architecture, allowing both commercial and public sector customers to share the same computing resources, subject to robust access controls. In Korea, all central and local government ministries, affiliated public institutions, and educational institutions (from primary schools to universities) are effectively prohibited from adopting cloud services offered by U.S. CSPs.

CSAP also does not comply with Korea's international trade commitments including the WTO Agreement on Government Procurement (GPA), the government procurement chapter of the U.S.-Korea Free Trade Agreement, and the WTO's Technical Barrier Treaty Agreement (TBT). Given Korea's participation in IPEF, it is noteworthy that CSAP is also in conflict with other widely accepted digital trade rules that are expected to be discussed under IPEF, including ensuring seamless cross-border data flows, prohibiting data localization, safeguarding against the forced use of local encryption modules, and prohibiting the forced disclosure of source codes.

While CSAP is currently an administrative guideline, the implementation of CSAP has become more complicated and institutionalized in recent months. The 2023 amendment of the Cloud Computing Act has upgraded CSAP as a statutory requirement for state institutions in need of cloud service where it was previously an administrative guideline issued by MSIT. In August 2022, the Korean government officially announced its roadmap to revise CSAP as a more flexible multi-tier impact level and implementation of CSAP's critical requirements like physical separation. With no concrete action plans unveiled at the time, the anticipated regulatory change is still uncertain. We encourage the U.S government to advocate for reforms to the CSAP program that would open the public cloud sector market to global cloud service providers.

Malaysia

Technical barriers to trade

The Ministry of Domestic Trade and Consumer Affairs (MDTCA) has stated plans for a mandatory safety approval program focusing on secondary batteries/consumer products. ITI has repeatedly requested from MDTCA a copy of the updated draft secondary battery standard and its certification process to allow ITI member companies sufficient time to provide feedback before the guidelines are released, but inquiries on the changes have not been answered. ITI understands that the program may be broadened in late 2021, but as of September 2022, communication with industry stakeholders has been minimal, raising concerns that there will be limited time for a robust consultation process. It would be helpful for the U.S. Government to clarify the upcoming scope and program requirements and work to ensure adequate notification and transition time.

The Malaysian Communications and Multimedia Commission (MCMC) announced new licensing obligations for data centers and cloud service providers to apply for a service provider class license (ASP(C) License) under the Communications and Multimedia Act 1998 (CMA 1998).

Services barriers

Bank Negara Malaysia's (BNM) Interoperable Credit Transfer Framework (ICTF) was finalized in March 2018 and came into effect on July 1, 2018. The ICTF applies to certain credit transfers, specifically payment services that allow a consumer to instruct the institution with which the consumer's account is held to transfer funds to a beneficiary, also known as push payments. In December 2019, BNM reversed a policy that would have only allowed a single operator, i.e., local network PayNet (partially owned by BNM), to process all domestic credit transfer transactions. This is a welcome development as it enables U.S. providers to compete on a level playing field, in alignment with Malaysia's WTO General Agreement on Trade in Services (GATS) commitments. However, payment providers have to obtain approval from BNM, which requires meeting conditions such as safeguards to protect and access data located offshore, enabling interoperability and reducing fragmentation of multiple providers and pricing transparency.

Mexico

Barriers to digital trade and electronic commerce

ITI has been tracking a number of legislative proposals in Mexico targeting Over-the-Top (OTT) services. In September 2020, Senator Ricardo Monreal presented a legislative project that seeks to reform the Federal Telecommunications Act and require a 30 percent local content quota for OTT platforms operating in Mexico. A local content quota for OTT platforms would seemingly violate Mexico's commitments under USMCA (Articles 14.10 and 19.4.1), as well as limit free expression and consumer choice, distort the growing audiovisual market, and stifle investment and competitiveness. The Senator subsequently presented a revised bill in February 2021 that seeks to establish a 15 percent local content quote. If this policy is enacted, Mexican audiences and creators would have fewer legitimate options for film and television content.

In addition, the Mexican government has shared a draft proposal for the audiovisual industry with several potentially problematic elements, including: requiring digital streaming platforms to use Mexican content classification (art. 26), creating a reinvestment requirement whereby operators of digital streaming platforms that provide their services in Mexico must allocate each year the amount equivalent to five percent of the profits that they report annually to the Ministry of Finance and Public Credit as a donation to the promotion of national cinema through the Mexican Institute of Cinematography (art. 26), and requiring a visible section with audiovisual content of national origin (art. 26).

Additionally, legislative language (Iniciativa con proyecto de Decreto por el que se REFORMAN y ADICIONAN diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión) under consideration in the Mexican Senate would establish new requirements for "relevant social network providers," such as securing pre-approval by the Mexican government for terms of services and applying limitations on providers' ability to terminate user accounts, among other requirements. These requirements would create significant barriers to the operations of ITI members in Mexico and raise questions under Mexico's trade obligations, in particular its commitments in the telecommunications chapter of the USMCA.

On September 8, 2020, former Secretary of Finance & Public Credit Arturo Herrera presented to the Mexican Congress the legislative project for the Government's Budget for 2021. Included in the proposal was the implementation of a "kill switch," an enforcement mechanism that the Mexican government initially proposed in their 2020 Budget against non-resident entities that do not comply with the application of the VAT on non-resident supplies of digital services to Mexican consumers. The "kill switch" was ultimately included in the Government Budget passed on January 1, 2021. While the Mexican government has reiterated that it does not intend to implement this mechanism, its inclusion in the 2022 Budget and again in the proposed 2023 Budget leaves open the possibility. Should the regime be applied, it would empower the tax authority to work with the telecom regulator to require internet service providers (ISPs) to block internet access to non-resident entities providing cross-border services. Such measures threaten the free flow of cross-border digital services trade, including digital services provided by U.S. tech companies. ITI continues to urge the Mexican government to amend this provision in a way that achieves its tax policy objectives and conforms with Mexico's international trade obligations.

Technical barriers to trade

Mexico is regulating the energy efficiency of products through a variety of duplicative and in some instances conflicting regulations. These include the Energy Transition Law (ETL), the subsequent Regulation of the ETL, official standards for specific products, and country specific tests and labels that impose additional costs and burdens on manufacturers. Mexican Metrology law, in concert with specific Mexican standards (NOMs), mandates unique and excessive annual testing requirements. As an example, globally, industry tests external power supplies once and only re-tests a product if it has been modified. Mexico's proposed Official Norm (NOM)-029 deviates from this regionally and internationally accepted practice and imposes significant burdens on industry.

Mexico has been working for a few years to update its product safety regulations for IT and electronic equipment. NOM-001-SCFI-2018 (Electronic devices-Safety requirements and test methods) was published in 2020 and industry eagerly awaits publication of the final NOM-019-SE-2020 (Information technology equipment and related apparatus, and office equipment). Meanwhile, Mexican Standards Agency (DGN) noted that it would not update an equivalency arrangement under which it recognized testing to U.S. and Canadian standards for product safety. This indication became reality in late 2020, as Mexico has since been unwilling to update the unilateral equivalency arrangement that had been in place for years to reference the most current NOMs. As a result of equivalency becoming invalid (once the updated NOM 019 is published and already the case for NOM 001), numerous products now require in-country testing and certification to Mexico's own product safety standards. To avoid expected bottlenecks and increased costs and delays at Mexico's local labs, ITI proposed that Mexico leverage its existing membership in the IECEE CB Scheme to update its standards and accept CB certifications and test reports in lieu of local testing and certification. These recommendations were rejected by Mexico. The refusal to accept international accredited test lab reports means that the transition time for NOM 019 is even more important. Industry is concerned that DGN will allow only 6 months of transition time, which is, in effect, only three months for industry to test and certify

products because labs typically take at least three months to adapt to a new standard. We request that USTR encourage DGN to give a transition time of at least one year before requiring certification to NOM-019-SE-2020 for new products.

In March 2020, Mexico published their Quality Infrastructure Law (QIL). ITI applauds the goals of the draft law to make the elaboration of standards more agile and flexible; reduce development time; and make processes efficient through the use of information and communication technologies and platforms. However, we have concerns about the QIL's compatibility with the USMCA's TBT chapter. The USMCA includes updated provisions with important specifications regarding international standards and conformity assessment and we believe this law should either reference or incorporate key elements of that language. ITI encourages more consistency with TBT and USMCA obligations in order to avoid disharmonization of previously understood standardization criteria. Keeping this consistency will encourage conformity to standards while promoting producer efficiency, which will facilitate the supply of products to the consumer market in Mexico. In particular, we have raised the following issues:

- The definition of "International standard" differs from the definition included in Chapter 11 of the USMCA, which simply states "a standard that is consistent with the TBT Committee Decision on International Standards." Further, Article 11.4 of the USMCA states that parties should refer to the TBT Committee Decision when determining whether there is an international standard. ITI strongly recommends Mexico reference this definition instead of the language as it is currently proposed in the law.
- ITI recommends that Mexico examine and incorporate the IECEE model as a best practice. Operated by the IEC, the IECEE CB Scheme is an international system for mutual acceptance of test reports and certificates dealing with the safety of electrical and electronic components, equipment and products. Under this scheme, a UL/Canadian certificate only needs to be updated if a hardware change is made to a product, and internationally accepted certification body (CB) reports do not have expiration date. Indeed, a CB test certificate is valid for as long as the certified product conforms with the initial certification. We believe this type of scheme would greatly benefit the Mexican market by allowing assurance of conformance to standards, while at the same time providing an efficient path for safe products to the Mexican market.
- The minimum effective date for NOMs, once published in the official gazette, is specified as 180 days (six months). In 2019, we saw several changes in import law and registration systems, which caused significant burden on industry in a relatively short timeframe. To enhance understanding of and conformity to published NOMs, ITI recommends a longer minimum effective date of 365 days (one year) after publication in the official gazette.

Mexico has responded that we will be able to comment on various requirements as aspects of the QIL are incorporated into regulation, but inclusion of a general emphasis on the need to ensure alignment between the QIL and the TBT provisions of USMCA in the 2023 NTE will further emphasize the importance of these matters.

ITI has asked Mexico's telecommunications regulator (IFT) and Ministry of Economy to examine the compatibility of their specific absorption rate (SAR) regulation, IFT-012-2019, with the WTO TBT Agreement and Chapter 11 and Annex 12-C of the USMCA. MRAs can help to alleviate the workload of local testing labs, reduce testing times, promote competition, and facilitate the access of Mexican consumers to the latest ICT technologies. We request that USTR examine the regulation and encourage Mexico to use MRAs to every extent possible.

Repair and refurbish operations are an important and environmentally friendly part of ICT product trade. ICT manufacturers often operate facilities in United States that refurbish and/or repair devices for further sale overseas, including in the Mexican market. In December 2020, Mexico's Ministry of Environment and Natural Resources (SEMARNAT) issued regulations that re-classified ICT devices exported to the United States for repair, re-use, or refurbishment as e-waste, and subsequently required Mexican export permits for these goods, creating barriers to trade in these products and a more circular economy.

Import policies

USMCA entered into force on July 1, 2020 and included positive outcomes for U.S. companies in the Customs chapter, including streamlined, simplified, and expedited border processing to help speed border clearance times and lower costs for low-value shipments. This included commitments by Mexico to implement new *de minimis* and informal clearance thresholds.

On May 27, 2021, Mexico's Tax Administration Service (SAT) published revised General Foreign Trade Rules that raised the informal clearance threshold to $2,500. The increase to $2,500 went into effect on June 26 for shipments valued at >$117. However, the Secretary of Economy (SE) still needs to harmonize its own regulations to allow for this change to be fully implemented, which has not happened to date. Specifically, the SE needs to update Section IX, Article 10 of the Annex 2.4.1, which still requires compliance with all applicable NOMs for those courier shipments with a value of $1,000 or more, which, in line with the recent changes to the SAT rules and the USMCA, should be updated to $2,500.

In addition, Mexico has published new regulations that increased import rates on shipments from the U.S. and Canada valued between USD $50-117 by 1 percent (from 16 percent to 17 percent). For non-USMCA shipments, the import rate was also increased by 3 percent (from 16 percent-19 percent) for shipments between USD $50-1000. These changes were made without warning or following appropriate protocols, and they became effective immediately. While this is a small increase, it appears to constitute a violation of the USMCA.

The approved 2021 Budget allowed the Secretariat of Communications & Transportation (SCT) and the Tax Administration Service (SAT) to increase reporting requirements. To implement these new reporting requirements, the SCT and SAT published regulations that requires a carta porte (transportation consignment note), which is an addendum to the invoices that document the origin and destination of goods transported inside of the country. As of September 30, 2021, this carta porte requires the incorporation of new and mandatory catalogues and information related to the goods, locations of origin, and intermediate points and destinations. Documentation must

also refer to the means by which they are transported (either road, rail, air, sea, river or multimodal).

These measures will increase the complexity of the business environment and the conduct of business and trade in Mexico and North America. ITI requests that USTR include this issue in the 2023 NTE and address it as soon as possible, as it creates an uncertain environment for U.S. exports to Mexico and is inconsistent with international norms.

Services barriers

Mexico continues to enforce a 2021 regulation which requires electronic payment fund institutions to maintain a business continuity plan in the case of disaster recovery that relies on either 1) a multi-cloud approach with at least two cloud service providers from two different jurisdictions, or 2) an on-premise data center in country that does not depend on the primary (foreign) cloud provider. The National Banking and Securities Commission's (CNBV) approval process is resource-intensive and burdensome for foreign cloud providers, whereas existing local on-premise data centers merely need to complete a shorter, simpler notification process. This de facto data localization requirement is in addition to an already complex and time-consuming process that electronic payment fund institutions face in order to gain regulatory approval to use offshore cloud infrastructure, whereas in country infrastructure enjoys an expedited process. The United States has raised concerns with the Mexican government that the requirements relating to use of cloud service suppliers by electronic payment fund institutions have a negative competitive impact on the business of U.S. service suppliers.

Mexican financial sector regulators – CNBV and the Central Bank of Mexico (Banco de Mexico) – have issued Provisions Applicable to Electronic Payment Fund Institutions (IFPEs). Article 50 of the Draft Provisions would impose data residency requirements on IFPEs that use cloud computing services (alternatively, the Article imposes reliance on a multi-provider scheme). Article 49 would establish an authorization model with a high degree of discretion and lack of transparency for the use of cloud computing services. These requirements to localize data run counter to the spirit, if not the letter, of USMCA's digital trade and financial services provisions. These regulations undermine U.S. financial services providers, which already face lengthy and uncertain approval processes from CNBV or Banco de Mexico in order to use secure, U.S.-based cloud computing services. Additionally, the regulation could negatively affect the adoption of cloud computing in the country and create an uneven playing field where U.S. cloud computing companies would be at a disadvantage with respect to local companies.

In 2014, the Mexican Congress amended the Law for the Ordering and Transparency of Financial Services (*Ley para la Transparencia y Ordenamiento de los Servicios Financieros*) to grant powers to the Central Bank of Mexico (Banxico), among others, to authorize the entrance of new competitors. The amendments were intended to introduce competition into the domestic processing market, eliminate potential entry barriers, and promote market development. The amendments also brought the two local and existing payment networks—Prosa and e-Global—under Banxico's oversight.

For decades, Prosa and E-Global, both owned by Mexican banks, have dominated domestic processing by developing and operating under a set of rules and standards specific to Mexico, known as Red MX (Mexico network). To date, Red MX is the only set of standards and rules recognized by the market and regulators. Even the current local rules, an industry agreement authorized by Banxico in October 2014 known as the Conditions for the Interoperability of Clearinghouses (CICC), rely exclusively on Red MX.

After more than two years of extensive consultations that have required significant investments in resources (USD $1.2M in consultancy services) and time from all payment networks participants, including local incumbents and U.S. entrants, an industry agreement to promote interoperability among different payment networks, known as Iniciativa 28, was reached in December 2018, but has yet to be implemented. The current regulatory framework still reflects the commercial situation as it existed before new (foreign) entrants were permitted in the domestic processing market, is unclear, and provides no mechanism for interoperability between new (foreign) and existing clearinghouses. In the face of this ambiguity, the current regulatory framework effectively requires new clearinghouses to be certified by Prosa and E-Global and to process domestic transactions exclusively under Red MX standards and rules. Without action by Banxico and the CNBV to resolve this ambiguity, U.S. payment firms will remain unable to operate in the market leveraging their own standards and rules, which are crucial for the deployment of their full array of services and demonstrating their competitive advantage vis-à-vis local firms. These elements of Mexico's domestic payments regime, individually and collectively, impede fair competition among EPS services suppliers and do so in a manner that favors domestic players. Indeed, the Mexican competition authority (COFECE) released on December 16, 2020 preliminary results of an investigation confirming that the existing market conditions do not provide effective competition in the Mexican payments industry and offer recommendations to COFECE's Board of Governors on actions to foster competition. However, the President of Mexico has not proposed new Commissioners for the Senate and, with the current vacancies, COFECE cannot enforce any measures.

We urge USTR to ensure that Mexico brings its domestic payments regime into compliance with its EPS market access and national treatment commitments under the USMCA, in particular by providing a fair, transparent, and level playing field so as to allow full competition among suppliers' service offerings.

Procurement

Mexico's National Digital Strategy as published in September 2021 includes provisions regarding data localization that could drive Federal Government cloud procurement to favor cloud providers with data centers in Mexico. It also favors procurement contracts derived from Framework Agreements already in place, which could have the impact of discriminating against providers without such agreements.

Other issues

While the Mexican government started to liberalize the energy sector in 2013, President Andrés Manuel Obrador López has implemented multiple amendments to the Law on the Electricity

Industry and Hydrocarbons Law to increase the market share of state-owned energy companies (Petróleos Mexicanos (PEMEX) and the Federal Electricity Commission (CFE)), with the stated intent of promoting Mexican energy self-sufficiency. Reforms to date have presented serious hurdles for companies seeking to connect to the electricity grid and purchase clean and reliable energy. These hurdles include directing energy consumers to purchase energy from the state-owned utility (CFE) and receiving disproportionate transmission infrastructure requests as part of the process to connect to the grid with the National Center for Energy Control (CENACE). Many of the infrastructure requests are actual recognized obligations of the Mexican State, that have simply not been met. Concurrently, the Mexican government has taken steps to prevent the private sector from effectively participating in the local energy market by revoking permits, delaying issuance of new licenses, and preventing companies from operating renewable energy facilities or off-grid generation. We understand the United States has raised concerns with Mexico in several instances, including through dispute settlement consultations under Article 31.4.5 of the USMCA. These discriminatory policies are impacting U.S. companies' ability to reliably and adequately source energy on the local energy market, especially as U.S. companies are pursuing clean energy targets.

New Zealand

Barriers to digital trade and electronic commerce

New Zealand's online safety legislation – the Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill – became law in February 2022. The Bill, which is framed in response to the Christchurch attacks of 2019, enacts two main changes: 1) the establishment of a notice and take down scheme for 'objectionable' online content backed by civil penalties; and 2) a new criminal offence for the act of livestreaming objectionable content. A parliamentary committee has just reported on the Bill, recommending (among other things) to make the Bill's claim of extraterritorial application more explicit, such that international services accessible by New Zealand citizens will be obligated to remove content that fits in the notably broad and subjective category of "objectionable," "regardless of whether an online content host is resident or incorporated in New Zealand or outside New Zealand."

Nigeria

Barriers to digital trade and electronic commerce

In August 2020, the Nigerian government published a draft Data Protection Bill. The Bill is intended to replace the existing Data Protection Regulation, issued by the Nigerian IT Ministry in 2018. The Bill is similar to many other data protection laws, but is unclear in its present scope and contains several requirements with the potential to increase compliance costs for entities operating in Nigeria. We understand the Nigerian government intends to pass relevant legislation by December 2022.

Key components of the draft Data Protection Bill:

- The scope of the bill is presently unclear, creating regulatory uncertainty for entities operating in the Nigerian market.
- Data breach notification obligations for both controllers and processors (to both individuals and to the regulator); requirements do not include any threshold for notification, potentially creating significant administative burden on organisations to notify every instance of unauthorised data access (whether or not there is a risk of harm to individuals).
- Legal mechanisms for cross-border data transfers are not set out fully in the present draft, potentially leading to regulatory uncertainty regarding organisations' ability to transfer data across international borders.
- Automated decisions currently require notification to the data subject whenever a "decision" is made about that individual "which produces legal or similar significant effects"; this has the potential to force all organisations to implement onerous notification systems to alert individuals on every occasion their data is used to determine the operation of that organisation's computer systems. We would recommend deletion, or to add a 'legitimate interest' exemption to this requirement.
- Requirement to identify a Data Protection Officer (DPO).
- Fines of up to approximately $23,000 USD or imprisonment for potentially up to five years for failing to comply.
- It is also unclear how the establishment of a Nigerian Data Protection Commission would interact with Nigeria's newly established Data Protection Bureau.

Taxation

Nigeria adopted a "significant economic presence" (SEP) measure through Finance Act, 2019 and the associated Order was published in May 2020; however, the measure applied retroactively to February 3, 2020. While it operates as an income tax, the applicability of the measure depends on a nonresident company's annual gross turnover in Nigeria from certain digital activities, such as providing goods or services through a digital platform and delivering streaming or downloading services of digital content. This approach contravenes longstanding international tax principles such as tax certainty and the internationally recognized definition of permanent establishment, and acts as a trade barrier to U.S. companies operating in the Nigerian market. ITI asks that USTR engage with Nigeria to seek withdrawal of the SEP measure and Nigeria's re-commitment to the multilateral project through the Inclusive Framework to address tax challenges of the digitalizing global economy. This is especially important as Nigeria has not lent its support to the OECD/G20 Inclusive Framework's October 8, 2021 Statement that commits participating governments to the removal of relevant unilateral measures.

Pakistan

Barriers to digital trade and electronic commerce

Pakistan issued in August 2021 a new draft of the "Personal Data Protection Bill" following an initial draft published in May 2020. The new version retains the prohibition on the cross-border transfer of "critical" personal data and the right to impose further restrictions on "sensitive"

personal data. Sensitive personal data includes financial data which is often routinely processed by businesses. The scope of "critical" personal data is not defined, and the proposed National Commission for Personal Data Protection would have extensive powers to introduce new regulatory frameworks which may create further blockers. Given the wide and open-ended definitions of sensitive and critical data, this proposal could seriously impede cross-border data flows and free trade.

Pakistan is also in the process of finalizing a Cloud First Policy. This policy would impose data localization requirements on wide and open-ended classes of "sensitive" and "secret" data. In the financial sector, the State Bank of Pakistan (SBP) prohibits financial sector institutions from storing and processing core workloads on offshore cloud. These data localization requirements are ineffective at enhancing the protection of personal data, and would significantly increase costs for U.S. firms, potentially deterring market entry.

In November 2020, Pakistan adopted the Removal and Blocking of Unlawful Online Content (Procedure, Oversight, and Safeguards) Rules. The government is currently re-drafting the Rules. The Rules apply to the removal and/or blocking of online content that is deemed unlawful on any information system. Local and international industry players have expressed concerns regarding provisions that would pose significant barriers to operating in Pakistan, including burdensome registration and licensing requirements, content restrictions, requirements that companies maintain a physical presence in Pakistan, and data localization. Pakistan periodically blocks access to internet services for hosting content deemed to be "blasphemous" or "immoral" or on grounds that such services can be used to "undermine national security." The Pakistan Telecommunication Authority (PTA) has also sent notices to U.S.-based social media platforms, threatening adverse action if those platforms did not remove objectionable content. Following the adoption in November 2020 of the Removal and Blocking of Unlawful Online Content (Procedure, Oversight, and Safeguards) Rules, Pakistan issued in October 2021 the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards), Rules 2021" (Rules) to supersede the 2020 version of the Rules. The Rules apply to the removal and/or blocking of online content that is deemed unlawful on any "information system." Local and international industry players have expressed concerns regarding provisions that would pose significant barriers to operating in Pakistan, including requirements to deploy mechanisms to monitor and block livestreaming content, remove content within short timeframes when ordered by the authorities, and provide data to authorities in decrypted and readable format.

Services barriers

In February 2020, the Ministry of Information Technology and Telecommunication (MOITT) posted on its website the Citizens Protection (Against Online Harm) Rules.[17] The Rules contain onerous requirements including forced local office presence; forced storing of user data within Pakistan; and new procedures that would contravene international norms around disclosure of user data and intermediary moderation of online content. The government announced in March 2020 that a committee led by the PTA would conduct an "extensive and broad-based consultation

[17] https://moitt.gov.pk/SiteImage/Misc/files/CP%20(Against%20Online%20Harm)%20Rules%2c%202020.pdf

process with all relevant segments of civil society and technology companies." However, a revised version of the Rules has not been circulated, and a broad-based consultation has not yet occurred.

Panama

Barriers to digital trade and electronic commerce

The Government Innovation Authority (AIG) of Panama published (09/10) resolution No. 52, which stipulates that all cloud services, mission-critical, or state-security databases, or sensitive institutional data of all Government Entities must be held in Panamanian territory by December 31, 2022.

Paraguay

Import policies

In addition to other measures previously listed in the 2022 NTE, Paraguay also requires homologation certificates issued by Conatel (Comisión Nacional de Telecomunicaciones) to import smartphones. Exacerbated by seasonal demands, importers have in some cases experienced extended approval times of more than 10 weeks, limiting their ability to import products to serve local demand.

Peru

Barriers to digital trade and electronic commerce

In May 2020, the Digital Government Secretariat of Peru released for consultation a draft of Emergency Decree 007 – Digital Trust Framework regulations. Peru's proposal includes:
(i) the creation of an accepted list of countries, which will indicate permitted countries for the cross-border transfer of data, even though the Peruvian Data Protection Law does not include such restrictions; (ii) the issuance of digital security quality badges for private companies, the specifications of which will be based on governmental cybersecurity certification, rather than widely used global security standards; and (iii) the creation of a national data center.

The proposal also includes broad definitions of digital services providers that do not consider key differences among such providers. The Data Protection Authority would be responsible for developing model contract clauses, which appear to expand upon requirements currently established under the Data Protection Law. The national data center would incentivize domestic data storage through the infrastructure development of domestic data center operations at which the Peruvian government would exercise control over data stored on-site.

Instead of pursuing data localization, we would ask that USTR encourage Peru to rely on the already approved Guidelines for the Use of Cloud Services for entities of the Public Administration, and endorse the use of international standards and best practices such as ISO 9001, ISO 27001, ISO 27002, ISO 27017, ISO 27018 and SOC 1, 2 and 3.

Import barriers

The U.S.-Peru Trade Promotion Agreement (the Agreement) entered into force on February 1, 2009. Under Article 5.7(g) of the Agreement, the parties established a de minimis, the value threshold below which no customs duties or taxes are charged on imported goods. The Agreement's de minimis threshold is set at $200. However, the National Superintendent of Customs and Tax Administration (SUNAT) has implemented restrictions to the number of express delivery shipments (three maximum) that an individual without a tax number (RUC) can do per year. Also, for individuals, it is uncertain if an individual has more than three shipments, these personal imports would be considered commercial and create new income tax obligations. Thus, the RUC requirement limits the ability for individuals to import goods for personal use and constitutes a trade barrier and a limitation to the use of express delivery shipments in Peru.

Services barriers

On July 11, 2021, the Secretary of the Peruvian Congress published a report that proposes to modify the Audiovisual and Cinematographic Activity Promotion Law. The document unifies two bills: the first (6257) would establish screen quotas, while the second (7465) proposes the creation of a Film Commission and the promotion of audiovisual productions. If implemented, the legislation would establish local content requirements and create a new incentive regime. Specifically, Article 20 states that the Ministry of Culture may set "annual rules on minimum percentages of exhibition and commercialization of Peruvian cinematographic works in any medium or system. This percentage must not exceed twenty (20 percent) percent of the total commercial and cultural works exhibited in the country during the same period of time."

Philippines

Barriers to digital trade and electronic commerce

The Philippines' national legislature has been considering regulation of all internet transactions through the proposed Internet Transactions Act (ITA) (House Bill 7805; previously House Bill 6122 and Senate Bill 1591). President Ferdinand Marcos Jr. has identified the ITA as a priority bill in the 19th Congress. The ITA seeks to introduce a new policy framework that would provide for regulation of non-resident online platforms and merchants, create obligations and undertakings for platform providers, shift the burden of policing online merchants to platform providers, and require substantial changes in the business model, product design, and function of platforms. The proposed mandatory registration and incorporation requirement for all online platforms and merchants that sell to Filipino customers is particularly notable, as it in effect mandates setting up permanent establishment in the country. The ITA would also impose solidary liability on platforms with their listed online merchants if the platforms do not perform the listed obligations therein. Imposing a fallback solidary liability framework would present onerous and far-reaching liability on platforms, disproportionate to the extent of their obligations under the proposed law. In addition, the wording of the provision imposing solidary liability does not present clear benchmarks for compliance by platforms, which would leave ambiguity as to the threshold for breach.

Earlier in 2022, the Department of Trade and Industry, together with other relevant government agencies, issued the Joint Administrative Order (JAO) No. 2022-01 for Online Businesses, which consolidates all rules and guidelines governing online commercial transactions. The JAO states that the laws applicable to physical or offline businesses are, as far as practicable, equally applicable to online businesses, particularly business-to-consumer and business-to-business e-commerce transactions. E-commerce platforms and e-marketplaces are required to verify the goods being sold on platforms comply with existing regulations, verify record of merchants selling on the platforms in terms of administrative or local law violations, and to take-down content, within three days, that violates regulations within the ambit of JAO signatories. E-commerce platforms and e-marketplaces shall also be held liable in the same manner as online sellers, merchants, and e-retailers when the latter commits any violation of the laws implemented by these rules.

Taxation

The House of Representatives reintroduced the Digital Value-Added Tax (VAT) bill (HB No. 372) in the 19th Congress, which would apply a 12% VAT on foreign providers of digital services to consumers in the Philippines. During the House Committee on Ways and Means deliberation on August 17, 2022, the Committee discussed introducing a provision requiring nonresident foreign corporations (NFRCs) to appoint a resident agent in the Philippines, which could have the consequence of creating a nexus for direct tax. The VAT bill will now enter the plenary session (2nd reading) and the House will conduct interpellation of the bill approved by the Committee.

Under the U.S. Income Tax Convention with the Republic of the Philippines, “taxation of business profits derived by a resident of the other country is governed 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." To access benefits under the tax treaty, the Philippines Bureau of Internal Revenue (BIR) requires that income payors file a request for confirmation (RFC) with the BIR. The BIR has issued guidelines to administer annual pre-approval, which comes with onerous documentation requirements which undermines the benefit of the existing tax treaty. The BIR also indicates possible penalties and criminal liabilities for non-compliance. There is significant ambiguity on how long BIR will take to review the RFC, and there is no guarantee of a positive outcome. Such requests have to be made by each and every income payor (customer) of U.S. non-resident service providers selling to the Philippines.

Procurement

While U.S. cloud service providers are active in the Philippines, they continue to face constraints that limit their participation, particularly in competing for government projects. While the rules in public sector procurement do not explicitly require a local partner, they effectively force foreign bidders to get local partners. For example, when selling cloud services to the public sector, a foreign provider must secure a license to do business in the Philippines from the Securities and Exchange Commission (SEC) (see Government Procurement Policy Board Resolution No. 14-2021). As U.S CSPs do not hold a license with the SEC, they are required to work with local partners.

The government procurement system in the Philippines generally favors Philippine nationals or Filipino controlled enterprises for procurement contracts. Republic Act No. 9184 or the Government Procurement Reform Act, in consonance with Republic Act No. 5183, adopts as a general principle the preference for Philippine nationals and corporations in the award of government projects. Also, under Commonwealth Act No. 138 (An Act to Give Native Products and Domestic Entities the Preference in the Purchase of Articles for the Government) and reiterated in Section 43.1. of the implementing rules of Republic Act No. 9184, the government procuring entity can award a contract to the lowest domestic bidder even if there is a lower foreign bid, provided the domestic bidder's bid is not more than fifteen percent (15%) in excess of the lowest foreign bid.

Russia

The global technology industry stands in strong support of Ukraine and will continue to work with the U.S., Ukrainian, and other governments around the world to ensure we are a partner and resource in support of Ukraine. We recognize that diplomatic and other efforts to address Russia's illegal invasion of Ukraine are rightfully driving the U.S. government's policy agenda with the Russian government. As such, the following proposed and implemented barriers to trade in Russia are presented in the context of cataloguing barriers and not necessarily for immediate action by the U.S. government.

Barriers to digital trade and electronic commerce

Federal Law N236-FZ, which imposes new requirements on internet companies that service at least 500,000 daily users in Russia, entered into force on July 1, 2021. In-scope platforms must establish a legal presence in Russia.[18] While the legal presence requirement did not enter into force until January 1, 2022, other elements of the law entered into effect immediately, in particular a requirement to register with Russia's telecommunications authority (Roskomnadzor) and a requirement to provide certain online forms allowing regulators and users to contact company officials. Among other requirements, foreign companies will also be required to install Russian Government-provided software that counts the users of the website or app. Failure to comply may result in very harsh penalties, ranging from a ban for Russian companies and/or users to advertise with such foreign platforms to full or partial blocking of a non-compliant website or app. The law, which applies exclusively to foreign companies, was adopted without any public consultation or opportunity for affected companies to provide comment.

Federal Law 242-FZ, which requires data collected on Russian citizens to be stored in Russia, came into effect on September 1, 2015. This law affects the normal business operations of all industries in Russia by imposing inefficient operational rules, particularly the requirement in Article 18 to store personal data concerning Russian citizens in data centers located in Russia. It appears that Roskomnadzor, the federal regulator responsible for implementing this law, has accepted mirroring of data – keeping copies of data within Russia rather than the more extensive

[18] https://sozd.duma.gov.ru/bill/1176731-7. *See also* https://www.reuters.com/technology/putin-signs-law-forcing-foreign-it-firms-open-offices-russia-2021-07-01/.

requirements of processing it in-country – to be compliant with the law. However, the vague language in the law could allow for blocking cross-border data flows in the future, lending to an uncertain business environment in Russia. Furthermore, even mirroring of data can be very costly to businesses, particularly SMEs, increasing barriers to entry for the Russian market. In addition, the federal media regulator has been empowered to block local access to the websites of non-compliant companies. Given the law's expansive scope, foreign companies without a legal presence in Russia, which might pay only a cursory attention to the Russian market, can be labeled data protection violators and blocked. In late 2016, Russia began conducting audits and fining companies for violations. In one high-profile case, this audit resulted in a U.S. internet company being blocked outright from doing business in Russia. ITI requests that the U.S. government continue to highlight this law and working with the Russian government to ease its requirements.

In January 2021, the newly imposed Anti-Censorship Act came into force in Russia, giving authorities power to block or throttle platforms censoring "socially significant information." A platform will be liable for censorship by the Russian government if it restricts access to such information, such as termination of Russian accounts as well as other content restrictions, including for those taken for trade compliance purposes. The definition of censorship is extremely broad, potentially covering every single restriction applied to content such as termination of Russian accounts as well as other content restrictions including for trade compliance purposes.

On December 2, 2019, the Russian government released Law No 425-FZ which requires the pre-installation of Russian software on select devices. Amended later in 2020, the law requires all technically complex, consumer facing products to have a select group of apps installed before being shipped for sale to consumers. In effect since April 1, 2021, the measure discriminates against U.S. apps and imposes discriminatory burdens on U.S. device manufacturers. Moreover, on July 31, 2021, Russia promulgated an order that expands the list of applications to which the pre-installation requirements apply and introduces additional search engine pre-installation requirements; these broader measures are scheduled to enter into effect on January 1, 2022.[19] ITI requests that this issue be raised in the 2023 NTE.

On March 18, 2019, President Putin signed laws No. 30-FZ and No. 31-FZ which are ostensibly aimed at prohibiting the spread of misinformation online. The laws target online information that presents "clear disrespect for society, government, state symbols, the constitution and government institutions," and encompasses online insults of government officials. Russian authorities can block websites that do not remove information that the state assesses to be inaccurate, and the law allows prosecutors to direct complaints to the government about material considered insulting to Russian officials, which can then block websites publishing the information.

[19] http://publication.pravo.gov.ru/Document/View/0001202108100022

Introduced in February 2019, the so-called Internet Sovereignty Bill took effect on November 1, 2019. The bill creates mechanisms and requirements for routing Russian web traffic and data through points controlled by state authorities, building a national Domain Name System, and providing for the installation of network equipment that would be able to identify the source of web traffic and block banned content.

On July 7, 2016, President Putin signed a package of laws (374-FZ and 375-FZ) known as the "*Yarovaya Amendments"* that amended Russian Federal Laws 126-FZ and 149-FZ. These amendments require "organizers of information distribution on the internet" to store the content of communications that they enable within Russia for six months. In addition, telecommunications companies must store metadata of all communications within Russia for three years, whereas "organizers," referring to internet providers, must store metadata for one year. If any of this data is encrypted, then companies must also provide encryption keys to the implementing agency, the Federal Security Service (FSB). These requirements are costly for companies operating in Russia, so much so that even domestic telecommunications companies have been in vocal opposition to the law, a rare event in the country.

Taxation

In September 2021 the Russian government announced an intent to tax foreign technology companies as part of a broader plan to support the development of its domestic technology industry. We understood the timeline for introducing such a tax measure to be November 2021. While details continue to be scant, USTR should urge the Russian government to forgo the introduction of a unilateral tax measure.

Procurement

Russia has set into motion new compulsory quotas for the procurement of certain products by public sector and state-owned companies. In particular, amendments to Laws 44-FZ and 223-FZ in July 2020 required these entities to purchase a minimum of 30-50 percent of their telecommunications equipment and data storage systems from domestic sources. Additional requirements relevant to state-owned companies include a 30 percent price preference for Russian radioelectronic products over foreign products in tenders (15 percent preference for other products); recommendations to use non-competitive procedures when purchasing products under national quotas; and recommendations that state-owned companies shift to Russian hardware and software as part of their digital transformation. Additionally, draft regulations on critical information infrastructure (CII) provide for the preferential use of Russian hardware and software by all CII companies in two-to-three years (the exact timeline is unclear).

Saudi Arabia

Barriers to digital trade and electronic commerce

The Communications and Information Technology Council of Saudi Arabia (CITC) issued the Cloud Computing Regulatory Framework in 2018, with revisions made in 2019. The rules contain a provision on data localization that may restrict access to the Saudi market for foreign internet services. The regulation will also increase ISP liability, create burdensome new data protection

and classification obligations, and require compliance with cybersecurity and law enforcement access provisions that depart from global norms and security standards. CITC would be granted broad powers to require cloud and ICT service providers to install and maintain governmental filtering software on their networks.

The National Cybersecurity Authority (NCA) 2018 Essential Cybersecurity Controls (ECC) framework states that data hosting and storage when using cloud computing services must be located in-country. The draft NCA 2020 Cloud Cybersecurity Controls (CCC) framework requires operators to provide localized cloud computing services, including storage, processing, monitoring, support, and disaster recovery centers. The requirement applies to all levels of data. Neither the ECC nor the draft CCC distinguish between data localization requirements for different levels of data classification, which conflicts with the 2018 Cloud Computing Regulatory Framework.

Finally, the Saudi Authority for Data and Artificial Intelligence (SDAIA) and the National Cybersecurity Authority are working to issue a data localization and processing mandate that would include financial services. Such a mandate would prevent the free flow of data and present a significant trade barrier for U.S. companies operating in Saudi Arabia.

Procurement

In January 2021, the Saudi government announced that it would ban any company which does not host its regional headquarters in Riyadh from winning a government contract. The measure is expected to be fully implemented in January 2024.

Singapore

Technical barriers to trade

For years, the Cybersecurity Agency of Singapore (CSA) has implemented the cybersecurity Labeling Scheme (CLS) for IoT devices as a voluntary scheme. However, in 2021, the CLS for Wi-Fi routers became mandatory for certain (level 1) devices. The CSA has provided a one-year transition period for implementation, making the scheme fully enforceable in 2022. Required labels are valid for a maximum of three years and must be displayed on both the packaging and the product. However, e-labeling is not an option and vendors must meet requirement to attach physical labels on the products, which could potentially present trade barriers due to the unique designs. Further, CLS is based on ETSI standard EN 303 645, which is not an international standard that can be interoperable across regions. ITI continues to encourage the CLS to adopt international standards and accept flexible labeling formats that accommodate ongoing innovation.

Sri Lanka

Import policies

Since May 2022, Sri Lanka has moved to restrict imports into the country, severely affecting the ability to upgrade telecommunications infrastructure, availability of mobile phones, availability

of raw materials, and availability of intermediate goods for apparel and other manufacturing.

South Africa

Services barriers

A moratorium imposed by the South African Reserve Bank (SARB) on the migration of domestic transactions from a local processing system operator to international card networks has been lifted as of October 1, 2021. The moratorium was imposed in 2013 and reinforced in July 2018 in order to mitigate against perceived sovereign risk. The SARB has been reviewing the status of the processing of domestic transactions.

In August 2019, the SARB published a policy position stating that: (1) payment system operators will require a SARB license to process domestic transactions using on-soil infrastructure; (2) issuing banks are required to process domestic transactions through payment system operators whose infrastructure is established and maintained in South Africa; and (3) the July 2018 moratorium restricting banks from contracting new volumes to be processed with international networks would remain in place until September 30, 2021. The SARB has indicated that the Payments Association of South Africa (PASA) will amend the Payments Clearing House System Operators (PCH SO) criteria and publish it by the end of Q1 2022. PCH SOs will be required to process (authorization and clearing) domestic retail transactions through infrastructure that is established and maintained in South Africa within two years of the effective date of the amended PCH SO criteria.

Previously, industry was asked to present SARB with a set of options to comply with the Policy Position, which would form the basis of a Draft Directive. The SARB chose one of those options and published the Draft Directive in December 2019. In addition to on-soil infrastructure, the Draft contained a clause that all data related to domestic retail transactions should be stored in South Africa. Public comments were due in January 2020 and since then, the SARB has held a number of conversations with various agencies, including the Competition Commission.

Taiwan

Barriers to digital trade and electronic commerce

While Taiwan's sectoral regulations do not openly mandate data residency requirements for public institutions' use of cloud services, certain regulatory phrasing establishes a preference for data localization (e.g., "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."). When viewed in conjunction with additional burdensome and ambiguous approval requirements, these preferences may have in effect created a *de facto* data localization requirement. Specifically, if an institution decides to seek approval for overseas outsourcing of cloud services, it must confront burdensome documentary requirements which may cause unnecessary compliance costs. Where a foreign enterprise is willing to bear this additional burden, the review process is very likely to be lengthy and unpredictable and the institution still

needs to maintain a local copy of "important" data.

In Q4 2019, the Financial Supervisory Commission (FSC) issued an amendment to the Regulation Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, and the Directions for Operation Outsourcing by Insurance Enterprises, the first management guidance on the use of cloud computing services by financial and insurance institutions. The amendments include several requirements that would make it difficult for financial institutions to use cloud computing services such as over-burdensome documentary requirements, ambiguous approval criteria, unclear approval timelines, and duplicative audit requirements, which increase compliance costs for financial institutions and CSPs.

Thailand

Barriers to digital trade and electronic commerce

In 2019, Thailand passed a controversial Cybersecurity Law that industry has criticized due to provisions that enable government surveillance. Under the law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency." This could enable internet traffic monitoring and access to private data, including communications, without a court order.

Technical barriers to trade

In 2022, Thailand's Office of the Consumer Protection Board (OCPB) notified requirements for products containing lasers to the WTO TBT Inquiry Point. In addition to several technical comments and a request for more transition time, ITI pointed out that several of the labelling requirements are not aligned with WTO TBT criteria for legitimate policy objectives, such as the protection of human health and safety, or protection of the environment. The notification requires date of manufacture "to help [consumers] make purchasing and usage decisions" and purchase price as part of the labeling requirements. However, consumer purchasing and usage decisions are not among the WTO TBT criteria for legitimate objectives. ITI recommended that OPCB remove items from the labelling requirements that do not align with the WTO TBT Agreement and instead align laser classifications, safety warnings and documentation requirements with the international safety standard, IEC 60825-1:2014. We appreciate the U.S. government's support in emphasizing alignment with WTO TBT criteria.

Turkey

Barriers to digital trade and electronic commerce

Introduced in May 2022, the draft omnibus "Law Amending the Press Law and Certain Other Laws" would amend several existing bills to require OTT providers to have in-country physical presence, adopt a vague definition for disinformation, and establish an enforcement framework that includes potentially banning ads and throttling traffic, among other changes. Foreign social network providers (SNPs) with daily access of more than one million, must have a real person representative that is a Turkish citizen and residing in Turkey. This person(s) would be expected

to have full technical, administrative, legal and financial authority and responsibility. The requirement would take effect six months after the legislation's publication date. Turkey's Information and Communication Technologies Authority (ICTA) would also have the authority to ban advertisements for up to six months if a SNP does not comply with the ICTA's content removal/access ban decisions. Other sanctions could include requesting the criminal judgeships of peace for bandwidth throttling at the rate of 50%, or up to 90% if there isn't enforcement within 30 days following notification. Administrative fines would be based on a company's global turnover. The Grand National Assembly of Turkey is actively considering the legislation now.

On July 1, 2022, the Turkish Parliament adopted amendments to the Regulation of Electronic Commerce, which will take effect January 1, 2023. [20] The Law introduced concerning authorities, such as the ability of the Ministry of Trade to conduct audits of technical information like companies' algorithms and retrieve any information the Information Technologies and Communication Authority may seek to finalize complaints. Additionally, firms that facilitate sales equaling or topping ten billion Turkish lira net ($538.3 million) annually and over one hundred thousand executed transactions will be required to obtain a license to operate in the country and renew that license when the Ministry of Commerce dictates. Firms with net transactions of more than 60 billion liras ($3.3 billion) are subject to additional restrictions regarding banking, transportation, and delivery. The law also restricts certain e-commerce providers selling goods of their own brand or brands with which they have economic associations.[21] E-commerce providers will also be subject to obligations to take down illegal content and ads, ensure information is correct, and obtain consent before using brands for promotions.

In July 2020, Turkey adopted the "Law on Amendment of the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications" (widely known as the social media law). The law requires social network providers with more than a million users to: (i) establish a representative office in Turkey; (ii) respond to individual complaints in 48 hours or comply with official take-down requests of the courts in 24 hours; (iii) report on statistics and categorical information regarding the complaints every six months; and (iv) take necessary measures to ensure the data of Turkish resident users are kept in Turkey. In case of noncompliance, social network providers face serious monetary fines and 50-90 percent possible bandwidth reductions to their platforms. While these amendments aim to regulate social network providers and enhance the obligations of hosting and content providers in order to protect individuals in the internet environment, the vague obligation of data

[20] https://www.mondaq.com/turkey/contracts-and-commercial-law/1218860/new-law-amending-the-law-on-the-regulation-of-electronic-commerce-in-turkey-a-brief-introduction and https://www.srp-legal.com/2022/07/22/the-law-amending-the-law-on-the-regulation-of-electronic-commerce-has-been-published-in-the-official-gazette/

[21] https://www.lexology.com/library/detail.aspx?g=4e0f3279-d48c-4f2e-a0e1-752e9a7abfb8 ("As such, if these goods are offered for sale in different electronic mediums, providing access between such is not permitted. However, this regulation will not apply if the brand owner's revenue from e-commerce is less than half of its total sales revenue, or if the platform in question solely offers items carrying the Intermediary's brand in the form of agency contracts or franchising. Moreover, periodic publications, books and e-readers are also exempt from this regulation.").

localization may require significant and costly operational changes for businesses. In addition, broad governmental discretion concerning content removal/access blocking decisions raises significant concerns around potential censorship and the hindrance of free speech of individuals.

The Presidential Circular on Information and Communication Security Measures No. 2019/12, published on July 6, 2019, introduces important security measures, restrictions and obligations with the aim of mitigating and removing security risks and maintaining the security of certain critical types of data. Article 3 of the Circular states that data of public institutions and organizations shall not be stored in cloud storing services, except for the private systems institutions or local service providers under the control of public institutions. In addition, information and data defined as critical by the Digital Transformation Office, such as population, health and communication registration information, and genetic and biometric data, are to be stored domestically.

The Law on the Protection of Personal Data (numbered 6698) permits international transfer of data under the following conditions: (1) when transferring personal data to a country with adequate level of protection; (2) when obtaining explicit consent of data subjects; or (3) given ad-hoc approval of the Data Protection Board to the undertaking agreement to be executed among data transferring parties. However, industry reports that conditions make it hard to transfer data under these frameworks. Turkey has not yet announced a list of countries that meet the standard of adequate level of protection. Further, the Data Protection Board has yet to grant approval to companies that have sought the ad-hoc approval.

Taxation

Since March 1, 2020, Turkey has implemented a digital services tax of 7.5 percent to be applied to companies that provide their services through the internet and do not have a permanent establishment in Turkey. The bill taxes revenue from a wide range of digital services and provides the President with broad authority for altering both the rate (up to double the current rate, or 15 percent) and threshold of the tax. Similar to other digital services taxes, the Turkish measure establishes dual thresholds based on global revenue and revenue from the supply of covered services in Turkey, which effectively limits the application of the tax to large multinational companies. ITI appreciates USTR's efforts that led to the January 6, 2021 release of Section 301 Report on Turkey's Digital Services Tax and strongly encourages USTR to continue reiterating to the Turkish government the importance of withdrawing the unilateral measure and finalizing a multilateral, consensus-based approach.

Services barriers

The Regulation on Information Systems of Banks, published on March 15, 2020, still requires banks and financial services to keep their primary (live/production data) and secondary (back-ups) information systems within the country. The Regulation establishes a framework for use of cloud services as an outsourced service, but only applies for services located in Turkey.

United Arab Emirates (UAE)

Services barriers

In the UAE, nationally controlled telecom services have consistently controlled access to, and quality of, foreign internet-based communications services. This control has created significant market access barriers in a key Middle East market for U.S.-based internet services and apps. However, despite acknowledging the negative implications for foreign services, UAE regulators have declined to intervene, and instead continue to insist that only national providers can provide these forms of communications services. Given the conflict that this presents with UAE's GATS commitments, ITI urges USTR to classify this issue as a market access barrier and to engage directly with UAE in addressing this barrier.

In addition, USTR should take similar steps to monitor and engage with regulators in neighboring markets, such as Morocco, Saudi Arabia, and Oman, where nationally owned telecom services have engaged in similar forms of service blocking.

United Kingdom

Taxation

Retroactive to April 1, 2020, the United Kingdom adopted in July 2020 a digital services tax that applies a 2 percent tax on revenue generated through certain "digital services activities" attributable to a UK user. A company is liable for the tax if it meets dual thresholds of 1) global revenue related to in-scope services exceeding GBP 500 million; and 2) revenue related to the UK sale of in-scope services after the first GBP 25 million. This approach contravenes longstanding international tax principles such as tax certainty and avoiding double taxation. While the measure includes a reduction of tax obligation by 50 percent in certain circumstances where the same revenue is subject to another DST, the UK digital services tax exposes U.S. companies to the risk of multiple taxation and presents a challenge for U.S. companies engaging with the UK market. ITI appreciates USTR's efforts that led to the January 6, 2021 release of Section 301 Report on the United Kingdom's Digital Services Tax and strongly encourages USTR to continue reiterating to the UK government the importance of withdrawing the unilateral measure and finalizing a multilateral, consensus-based approach.

In February 2022, HM Treasury initiated a public consultation to solicit feedback on whether the United Kingdom should pursue an "online sales tax" (OST) as a means of reducing business rates for brick-and-mortar business models in the UK. The structure of the potential tax was not identified in the consultation, but at its core, the measure would be a unilateral, gross-based tax that is targeted at specific elements of a digitalizing economy. While HM Treasury has not publicly announced a decision in response to the consultation, USTR should emphasize that taking such an approach would challenge the OECD's consensus that it is not feasible to ring-fence the digital economy, conflict with the ongoing multilateral negotiations in the OECD/G20 Inclusive Framework, risk double taxation, and erect a barrier to U.S. companies' engaging with the UK market.

Uganda

Technical barriers to trade

Historically, Uganda had been using the Pre-shipment Verification of Compliance (PVoC) program common in several countries in Africa (Nigeria, Rwanda, Tanzania, and Zambia). However, in late 2021, Uganda proposed marking, import clearance, and market surveillance regulations that are redundant and would impose trade barriers. For example, the proposed regulation would require a permit to apply a mark that is specified in the Distinctive Mark regulation of 2018, in addition to the requirements of the PVoC process. ITI asked Uganda to exempt all ICT equipment, or at least equipment imported for business to business (B2B) sales and professional use, from the proposed regulations, as these items are already reviewed for compliance under the PVoC process. ITI also recommended that including an option for electronic-labeling, or e-labeling to display regulatory and other important information to consumers and regulators more effectively and efficiently than physical labeling. In addition, Uganda's proposed regulation did not indicate an option for using alternative foreign accredited test labs, and so ITI requested that Uganda base its technical requirements on international standards (IEC and CISPR) and accept foreign test lab reports less than 5 years old from accredited test labs. As of the date of this report, industry has received no response from Uganda on our submitted comments. We would appreciate the U.S. government's assistance in achieving a response and follow-up from Uganda, in addition to emphasizing our points to help avoid barriers to trade.

Vietnam

Barriers to digital trade and electronic commerce

On August 15, 2022, the Vietnamese government issued Decree 53/2022/ND-CP, an implementing decree for the data localization provisions of the 2018 Cybersecurity Law. Decree 53 entered into effect on October 1, 2022 and contains concerning provisions, including that foreign and local companies are subject to different data localization requirements, and without clear scoping definitions. The decree also lacks details on how domestic enterprises may comply, and may cause domestic entities to discriminate against using foreign service providers to avoid the risk of non-compliance. For local Vietnamese companies, the requirements in Decree 53 entered into effect immediately on October 1, 2022, and ambiguous compliance standards may trigger non-Vietnamese companies to enter into scope of the domestic companies. Local service providers include foreign invested enterprises established under Vietnamese laws who perform activities of collecting, exploiting, analyzing, and processing data that includes personal data of service users in Vietnam, data generated by service users in Vietnam, and data on the relationships of service users in Vietnam. Companies that fall under the "overseas entity" designation may be required to store data and to have a presence in Vietnam if (1) the Ministry of Public Security deems the services provided by the overseas entity violate the Cybersecurity Law; and (2) the Department of Cybersecurity and High-Tech Crime Prevention has sent a written notice to the entity, but the entity fails to adequately comply. In the instance that an overseas entity receives a request from the Ministry of Public Security to localize data, the company will have 12 months from receipt of the request to comply. Further, given the broad drafting of Decree 53, there is also lack of clarity on the applicability of data localization for foreign companies (i.e., a subsidiary of a foreign company incorporated in Vietnam could be considered

a domestic company under Decree 53), and the extent of the localization requirement (i.e., whether mirroring is allowed, or if data is not allowed to leave Vietnam). If all domestic companies are required to localize data under this implementing decree, U.S. cloud service providers and software service suppliers will be unable to sell services in Vietnam unless they build local data centers or localize their software data, which serves as a market access barrier that favors local telecommunications and cloud providers.

The 2018 Cybersecurity Law, finalized in June 2018 by the Ministry of Public Security, retains problematic language mandating data and server localization, severe criminal penalties for violations of the law, and broad requirements for various businesses and platforms to closely monitor and report information to the Vietnamese government. Such requirements can do great harm to businesses and, as observed in many of Vietnam's ICT measures, disproportionately affect foreign businesses as well as SMEs. In addition to Decree 53 described above, the Ministry of Public Security released the "Draft Decree on Cybersecurity Administrative Sanction" on September 20, 2021. This Draft Decree, yet to be finalized, lays out administrative violations, penalties, and remedial measures applicable to both Vietnamese and foreign companies. However, the decree also includes sanctions for violating the requirements set out in the Draft Personal Data Protection Decree and indicates that companies that fail to store data or establish a branch or representative office in Vietnam (Article 26.3 of the LOCS) may be sanctioned. This imbalance will disproportionately impact the ability of non-resident firms, in particular hyper-scale CSPs, to do business in country.

In February 2021, Vietnam's Ministry of Public Security (MPS) issued its first comprehensive set of personal data protection laws with an effective date of December 1, 2021. Among a variety of concerns around definitions and the scope of the law, Article 21 of the Draft would impose strict restrictions on cross-border transfers of personal data out of Vietnam and require the retention of original data onshore. The impact of such limitations on the transfer of personal data could be severely detrimental for businesses operating in Vietnam. In particular, the requirements state that businesses must receive written approval to be obtained from the Personal Data Protection Committee (PDPC), allow for annual assessments or audit-like exercises from the PDPC, and receive a granted document in order to prove the recipient country's level of protection. ITI instead recommends other cross-border data transfer alternatives, including standard contractual clauses, binding corporate rules, codes of conduct, and mutual recognition frameworks (i.e., APEC Cross border Privacy Rules). Finally, ITI is concerned about the short timeline to implement such a wide-ranging and comprehensive set of guidelines for personal data. Industry has not received further information on updated drafts since the release of the first draft Decree of the Personal Data Protection Law, for which ITI provided comments. We understand the latest draft is under review by the Politboro and will then be sent over to the Prime Minister for issuance of the PDP decree, now expected in late 2023 or early 2024.

Vietnam continues to consider or implement restrictive forced localization measures. First among them is the Ministry of Information and Communication's (MIC) *Decree on Information Technology Services* (Decree No.72/2013/ND-CP). This law requires every digital service or website to locate at least one server within Vietnam. This presents significant barriers for SME

market entry without providing any benefit to Vietnam's economy or consumers. In May 2020, MIC proposed changes that would include a new set of regulations on cross-border transfer of public information, give the government broad authority to force foreign compliance with take-down requests (within a window of 48 hours), and oblige domestic telecom firms to suspend service of foreign companies who fail to comply with take-down requests. In July 2021, Vietnam's Ministry of Information and Communication (MIC) released new draft amendments to Decree 72 on internet services which expands its scope to cover data center and cloud services. Such requirements are overly stringent and difficult to comply with, and specifically target foreign companies. After completing public consultations in September 2021, MIC has submitted the draft to the Office of Government (OOG) for review by OOG and then Cabinet members before finalization for issuance, expected in Q4 2022 or early 2023. ITI requests that the U.S. government again include this issue in the 2023 NTE.

In addition, the MIC *Law on Network Information Security* (LONIS) contains multiple troubling provisions regarding commercial cyber security products. This law appears to require source code disclosure of encryption software, encryption key surrender, and the surrender of proprietary trade secrets of cyber security products. In addition, broad requirements to cooperate with the government and obtain licenses in order to sell products within Vietnam could be implemented in a discriminatory manner. The first implementing regulation (the *Decree Guiding Law on Cyber Security*) contains broad import-export and business licensing and certification requirements on a wide variety of commercial ICT products containing cryptographic capability (even when encryption or cryptography is not the ICT product's main intent), and strict local presence requirements for providing cybersecurity services. While the Government of Vietnam later shelved the draft decree, this may always be reconsidered as Vietnam seeks to further develop its cybersecurity regime. ITI requests that the U.S. Government remain vigilant in watching this or any other data localization requirements that may appear in Vietnam in the future.

On June 3, 2020, Vietnam's Prime Minister signed Decision 749/QD-TTg, which announces the country's National Digital Transformation Strategy by 2025, and specifically calls for the introduction of technical and non-technical measures to regulate cross-border digital platforms. The MIC has subsequently issued Decisions 1145 and 783 to announce a local cloud standard and cloud framework, respectively, which set forward cloud technical standards and considerations for state agencies and smart cities projects in favor of local private cloud use. These decisions appear intended to create a preferential framework for domestic CSPs. Furthermore, the MIC Minister has made public statements noting that "as Vietnamese firms are getting stronger hold of physical networks, [Vietnam] must do the same for cloud computing and digitalization infrastructures […]".[22] While these standards are technically "voluntary," in practice, industry is concerned that their adoption by the Vietnamese public sector will render them *de facto* mandatory.

Taxation

The Tax Administration Law, effective July 1, 2020, taxes cross-border e-commerce and other

[22] https://vietnamnews.vn/economy/717123/data-must-stay-in-vn-says-minister.html

digital services. The Ministry of Finance had postponed implementation of Circular No. 40/2021/TT-BTC, which will mandate that cross-border digital service providers register, declare, and pay taxes (VAT and corporate income tax). In September 2021, the Ministry of Finance issued Circular 80[23] providing guidance on Law on Tax Administration and its Decree 126. 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 calls on the above digital suppliers to file dossiers for applying relevant tax treaty obligations to avoid double taxation at the same time as filing quarterly tax returns, but it is unclear how the suppliers, for whom the sales revenue are withheld by their buyers or commercial banks in the country, would claim a tax treaty's benefits. This onerous procedure coupled with the deemed tax rates will further complicate tax obligations for cross-border service providers and conflict with international taxation rules.

Technical barriers to trade

Generally, new MIC requirements have provided unreasonably short transition times, and some important measures were not notified through the TBT Inquiry Point (such as the publication of QCVN 127:2021/BTTTT). ITI saw several important improvements in 2022 and we thank the U.S. government for their support in achieving these. We received from MIC important confirmations on scope of standard, acceptance international test reports for QCVN 127 and 129 and updated 5G instructions allowing a self-declaration of assessment (SDoA) internally accredited test reports for QCVN18:2014. ITI continues to engage with MIC and MOST through the TBT Inquiry Point when measures are notified. We have consistently made several requests with respect to promulgation of current and new regulations and standards in Vietnam: (1) allow existing type approval (TA) certificates to be valid until expiration of the TA certificates; (2) accept TA applications to new standards ahead of the enforcement (entry into force) date; (3) extend the effective date of any QCVN to allow one year from the effective date of the standard to show conformance; (4) accept international test reports from labs accredited by peer-reviewed international accreditation bodies (such as A2LA and NIST); and (5) notify the WTO TBT Inquiry Point with clear requirements and ample time for robust stakeholder engagement. Further U.S. assistance in persuading agencies to implement these practices, respond to requests for clarification, notify to the WTO TBT Inquiry Point, and implement reasonable timeframes would be beneficial.

Import policies

The Government Cipher Committee (GCC) requires that the import and export of any product containing cryptographic functionality obtain specific permitting and licenses. Importers and Exporters entering IT products with data encryption capabilities must obtain Cryptography Trading License (CTL) and Cryptography Import License (CIL). Time periods for obtaining CTLs and CILs are significant – taking approximately six months to obtain. The process also requires

[23] See https://thuvienphapluat.vn/tintuc/vn/thoi-su-phap-luat/chinh-sach-moi/37945/thong-tu-80-2021-tt-btc-huong-dan-luat-quan-ly-thue-nd-126-2020

detailed information alongside the application, including detailed product information, a defined technical plan, information regarding the cryptographic function of the equipment, and information regarding local personnel. In application of these requirements, the GCC routinely inquires to a degree of technical detail that requires engagement by local personnel and technical experts, further delaying the application process and resulting in inconsistent application of approval processes. These burdensome requirements, and their routine follow-ups, limit the ability for companies investing in Vietnam to import critical hardware. The use of HS codes to identify products subject to the licensing regime covers a broad scope of products, some of which may not be relevant for the licensing regime. The HS system was designed to record trade activity and for the collection of duties and taxes, and it does not have the granularity needed to differentiate the various properties of each product regulatory scope.

We recommend instead that Vietnam adopt the ECCN (Export Control Classification Number) classification under the Wassenaar Arrangement that would provide a more granular level of classification that is related to the cryptographic function of products.

In addition to the GCC import licensing requirements, GCC recently issued Decree 23/2022/TT-BQP on civil cryptographic products to be additionally subject to in-country testing and certification. This certification process for civil cryptographic products by GCC is independent and separate from another overlapping certification process for wireless/Bluetooth/radio transmission products run by the Vietnam Telecommunications Authority (VNTA) under the Ministry of Information and Communications (MIC). Telecommunication equipment often have both radio transmission capabilities and civil cryptographic functions and hence fall under the scope of both certification processes. Although both agencies have similar objectives (e.g., safety and quality assurance of telecommunication equipment), they use completely different test standards such that the test reports for one certification cannot be used for the other. The duplicative and inconsistent requirements lead to unnecessary delays and increase in cost for imports into the country.

Further, GCC has decided not to adopt an incremental process towards the implementation of Decree 23 to start with a small scope of covered products and increasing it over time to a larger scope, but instead chose to immediately require all products supporting security functions (IPsec and TLS – the standards implemented in most network and ICT products) to be covered, even when they do not presently have any accreditation laboratory within Vietnam to undertake such evaluations. Given the impractically and the duplication with VNTA, this GCC requirement for testing should be removed from the import requirements.

Vietnam currently prohibits the import of refurbished products into the country, even when they are supported by warranty from the product principal vendor. This presents a particular challenge for products that have reached end-of-sale and are no longer being produced as new products, but they maintain requirements for warranty support or replacement by users in Vietnam. For other products still in manufacturing production, refurbished products also help support the circular economy and provide more cost-effective alternatives to users in Vietnam. Such refurbished products cannot be imported into Vietnam.

Services barriers

On August 19, 2020, the MIC released for public consultation a draft Decree to amend the Decree 181/2013 (guiding the implementation of the Law on Advertising). The draft seeks to regulate advertising content and has expanded Decree 181/2013's scope of application to include Apps and social media. The draft lacks clarity on definitions, procedures, and restrictions; imposes onerous reporting requirements; and obligates providers to actively manage ad content and placement. We urge USTR to seek a removal of all clauses in the draft that have overlapping applicability in other laws to avoid confusion, duplication, and unclear reporting requirements.

In recent years, the Government of Vietnam and State Bank of Vietnam have issued several policies and regulations intended to support the uptake of digital payments, including measures to cultivate the National Payments Corporation of Vietnam (NAPAS). A November 2019 revision to Circular 19/20178/TT-NHNN helpfully limits requirements to route transactions through NAPAS to domestic card present transactions only and extends the implementation deadline to January 2021. International payment companies met this deadline and are routing domestic card present transactions via NAPAS to comply with the regulation.

In July 2020, Vietnam issued a draft amendment to the Non-Cash Payment decree that includes the following changes: removes regulations on mobile money; removes the 49 percent cap on foreign ownership for an intermediary payment service; and allows commercial banks and branches of foreign banks to join international payment networks contingent on meeting requirements stipulated in Article 26 and approval by SBV. Article 26 appears to require existing and new clients of U.S. electronic payments companies to obtain written approval from SBV in order to continue doing business with U.S. electronic payment companies. Financial switching and electronic clearing service providers are allowed to connect to U.S. electronic payments companies only after meeting requirements as stipulated in Article 34 of the Decree and being approved by the SBV. These measures would appear to require NAPAS to obtain written approval from the SBV to connect to U.S. electronic payments companies. It is expected that the amendment to the non-cash payment decree will be passed before the end of 2021. We urge USTR's continued close attention to developments in this space, and the opportunity for close consultation with private sector (both domestic and international).

Zimbabwe

Taxation

The Finance Act No. 1 of 2019 introduced measures providing for the taxation of non-resident e-commerce platforms and satellite broadcasting service providers. Under these provisions, effective January 20, 2020, any amount received by or on behalf of an e-commerce platform or satellite broadcasting service provider domiciled outside Zimbabwe from persons resident in Zimbabwe are treated as income from a source within Zimbabwe and subject to tax at a rate of 5% if the revenue exceeds a threshold amount of U.S. $500,000 (ZWD 1 million) per year.