ITI Promoting Innovation Worldwide

October 29, 2020

ITI Response to USTR Request for Public Comments to Compile the National Trade Estimate Report (NTE) on Foreign Trade Barriers

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.

In the U.S.-Mexico-Canada Agreement's (USMCA) digital trade chapter, USTR established a model for ambitious commitments to counter barriers to digital trade on which it has continued to build, including with the 2019 conclusion of a bilateral Agreement on Digital Trade with Japan that enshrines strong commitments to maintaining open digital trade among two leading innovation economies and provides an example to which third countries should aspire. Active U.S. engagement in the World Trade Organization's (WTO) Joint Statement Initiative (JSI) on E-Commerce has proven essential in advancing negotiations toward a commercially meaningful plurilateral outcome that would provide a much-needed update to the framework of rules governing how commerce is to be conducted in the global, data-driven economy.

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 – impeding 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. The U.S. tech sector is likely to come under continued pressure as governments around the world craft and implement new and potentially restrictive governance approaches to data, digital services, and new technology.

ITI appreciates USTR's openness and responsiveness to discussions about the growing set of trade-related issues that the tech sector faces in foreign markets. Building on notable progress in recent years, the 2020 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 2021 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 encourage USTR to prioritize work on digital issues in the following ways:

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

1. **<u>Take action against digital trade restrictions that inhibit greater trade in technology products and services</u>**. U.S. trade officials must 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, source code, algorithms, or proprietary information relating to cryptography.

   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. We welcome, for instance, 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, services, or both – be based on global, industry-driven, voluntary consensus standards. This is particularly relevant as economies increasingly look to standards- and certification-based approaches to the regulation of new technologies. Continuing to address these items through direct government engagement as well as through the development of new rules in bilateral and plurilateral negotiations 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. **<u>Enforce U.S. trade agreements to ensure U.S. companies and workers can compete fairly</u>.** 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 U.S. industry. We acknowledge legitimate grievances with respect to the 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, unilateral digital taxation measures. 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.** Building on the achievement of the U.S.-Japan Agreement on Digital Trade, we strongly encourage USTR to expeditiously pursue similar digital trade commitments with viable third countries, including those with which USTR has regular meetings through trade and investment framework agreements (TIFAs) and comparable bilateral and regional engagement mechanisms. Doing so will have the dual benefit of promoting U.S. digital exports into key third-country markets, while broadening international acceptance of the most ambitious commitments on digital trade. ITI stands ready to actively support such engagement, which will further the United States' ability to craft inclusive, state-of-the-art rules governing trade in the modern global economy, to the benefit of U.S. exports, industry, and consumers.

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 designate a senior official responsible for digital trade with a status and mandate comparable to Ambassador-level positions for agriculture and intellectual property, and to add resources at all levels of the agency. 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 millions of 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

Since 2009, the government of Argentina has applied a 21 percent Value Added Tax (VAT) on information technology and electronic products, including mobile phones, cameras, and tablets produced outside the Special Customs Area within Tierra del Fuego province. Coupled with remaining customs duties on ICT products, the region-specific exemption of this VAT creates a significant distortion for foreign companies assembling final products outside of the Special Customs Area. With respect to ICT goods market access, while Decree 117/2017, issued on February 17, 2017, eliminated the 35% duty on imports of a number of electronic devices effective April 1, 2017, and the 12% import duty on electronic components as of February 21, 2017, tariffs remain on other products, including mobile phones. We urge the government of Argentina to expand and make permanent these tariff exemptions, as well as join the WTO Information Technology Agreement, in order to make technology products affordable and accessible to all and advance Argentina's digital transformation agenda.

Similarly, Argentina's decree 690/20, which declared ICT services to be essential public services, thereby changing the regulatory framework for internet, television, and mobile phone services in Argentina, poses significant challenges for ITI's member companies. We share the important goal of universal access; however, the essential services designation will create limitations, such as price controls and increased state intervention, that impede competition and innovation needed for a dynamic and growing ICT sector. As the decree is written, we are concerned Argentina could be advancing a law that would be out of step with international standards, subject to challenge under global trade rules, and jeopardize new investments in the ICT sector at a time when they are most needed.

Over the past twelve months, the Argentine government has applied a series of capital controls and new tax measures to the consumption of imports which have the effect of making 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% tax ("PAIS tax") on the purchase of foreign currency and purchases made online invoiced in foreign currency, among other things. On September 16, 2020, the Central Bank introduced a new 35% 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 products and services to Argentine customers.

Australia

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 issued his report in July 2020, which found that the law had largely succeeded in protecting Australians and did not require any major revisions. The Government is in the process of assessing the recommendations and will respond later this year.

The Criminal Code Amendment (Sharing of Abhorrent Material) Act was passed quickly through Australia's Parliament in early 2019, in response to the live-streamed mass shooting in Christchurch, NZ. The government did not offer a public consultation period, and several provisions of the law targeting the removal of online terrorism content are ambiguous and potentially overly broad. The law's wide-ranging provisions do not adequately consider different business models of technology companies or their varying capabilities in taking down content. Additionally, expectations regarding information that companies should provide to Australian law enforcement and the prescribed timeline remain quite vague.

In August 2020, the Australia Competition and Consumer Commission released a Draft Media Bargaining Code to address perceived imbalances in financial arrangements between news media publishers and digital platforms that may feature news content. The Code not only requires digital platforms to carry domestic Australian news content but would also require U.S. digital companies to transfer revenue to Australian competitors and disclose proprietary information related to private user data and algorithms. It explicitly and exclusively targets two U.S. companies without any indication of the selection criteria for these companies and their various services, or whether similar criteria was or will be applied to companies in or outside of Australia. The Code also accords the Australian Treasurer with unfettered discretionary power to designate other companies to which the Code should apply. The draft Code would impose discriminatory and burdensome responsibilities on U.S. companies where Australian, Chinese, Japanese, European, or other third-country technology businesses would not incur the same responsibilities. In solely targeting U.S. companies, the Code conflicts 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).

Industry continues to have copyright-related concerns in Australia, including as concerns Australia's commitments with the United States to provide liability limitations for service providers. The most recent amendments to Australia's 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.

Bangladesh

Industry has serious concerns about Bangladesh's proposed actions to restrict a number of chemical substances through classification under its Hazardous Waste (E-Waste) Management Rules, 2019. These actions were notified to the WTO TBT Committee on February 20, 2020 (see Notification G/TBT/N/BGD/3). The draft rules seem to deviate significantly from globally recognized regulations such as current Restriction of Hazardous Substances (RoHS) requirements. Working with industry partners, ITI submitted comments in response to this notification through both the U.S. and EU TBT Enquiry Points. We received notification that Bangladesh would extend the comment period through June 30; however, we have received no further indications of modification of the proposed rules or when they may ultimately enter into force.

As part of the proposed changes, Bangladesh is considering the restriction of Antimony trioxide, Beryllium metal / Beryllium oxide (Beryllia) / Copper beryllium alloys, nickel, "liquid crystals", Polyvinyl chloride (PVC), Mineral wool, Refractory Ceramic Fibers and TBBPA in electric and electronic equipment (EEE). These materials have been evaluated by the European Union (EU) and other countries and are not restricted under any current RoHS-like requirements. In fact, no exemptions seem to be included for mercury, lead, and cadmium for applications for which there are no technically or scientifically available alternatives and/or where the reliability of substitutes is not ensured, and/or where the total negative environmental, health and consumer safety impacts caused by substitution are likely to outweigh the total environmental, health and consumer safety benefits of their use. Some of the proposed restrictions impact substances that are commonly used in EEE. Exclusions for substances required for infrastructure-critical equipment (e.g., power generation equipment and electrical products necessary for that equipment to be used in a reliable and durable manner) should be accommodated. If the final Rules do not include critical exemptions for these substances, the ICT industry is concerned that it may be difficult, if not impossible, to produce EEE in Bangladesh.

Industry recommends that the Bangladeshi authorities thoroughly assess the potential impacts of the proposed restrictions by studying efforts underway in other jurisdictions across the globe to manage these substances, with a goal of aligning Bangladesh's requirements for critical elements with those in existing globally-recognized regulations. As a general matter, we strongly recommend that Bangladesh take a risk-based approach in its analysis of the proposed restrictions. Doing so would align with Bangladesh's general requirements under the WTO Technical Barriers to Trade (TBT) Agreement, and would ideally serve to prevent the emergence of costly technical barriers to trade stemming from divergences between Bangladesh's proposed approach and that of advanced regulatory systems across the world.

In addition, it is indispensable to the recycling of end-of-life EEE that adequate infrastructure be in place for all stages of transportation, storage, dismantling, recycling and disposal. In that regard, our members also recommend that Bangladesh thoroughly review the infrastructure currently available before requiring mandatory recycling. Effective implementation of extended

producer/manufacturer responsibilities (EPR) might not be feasible if recycling is mandated for a wide range of product categories without the necessary infrastructure in place. Sustainable product take-back schemes require participation or buy-in by all relevant actors including: *consumers* (who will need to return products to designated centers), *local waste management authorities* (who have access to existing waste management infrastructure), *the national government* (which presumably would need to provide funding and a legislative framework), *and manufacturers/producers* (who would need to be willing to finance product takeback programs and implement safe and responsible recycling programs). Shared responsibility by all actors is necessary for take-back and recycling schemes to be successful.

As a general matter, the amount of time and work required for effective global awareness and implementation of requirements by stakeholders at large, including but not limited to businesses and public authorities, should not be underestimated. Bangladesh should also ensure that it includes adequate transition periods from when regulations are ultimately adopted to when they go into force.

Finally, as the Government of Bangladesh and Bangladesh Bank prioritize digital payments as a conduit for financial inclusion for Bangladeshi citizens and small businesses, we urge USTR to ensure that any forthcoming regulations or policies allow for the full participation of U.S. payments firms on a level playing field in the market. A primary concern is Bangladesh Bank's position as both regulator and market participant in the National Payment Switch (NPSB), a state-owned domestic competitor. In recent years, Bangladesh Bank has introduced several draft policies that would impose requirements to route certain payment transactions over local infrastructure, as well as require all cards in the market to bear the logo of NPSB's brand - although these regulations have been held in abeyance. We ask that USTR remain vigilant of these policies and any regulations – including pricing interventions – that may favor use of local brands, and urge Bank of Bangladesh to consult with U.S. payment companies as it develops policies intended to facilitate a robust, secure, and inclusive ecosystem for digital payments, e-commerce, and financial inclusion.

Brazil

ITI remains concerned about the data localization requirement for public cloud in GSI Portaria 9 of March 2018. This requirement sets a troubling precedent for data localization that has no justification for security or government access. ITI encourages Brazil to take a more targeted approach, identifying which specific types of sensitive government data need to be stored locally, rather than requiring all data to be stored in Brazil and upending global and regional supply chains and services contracts.

Brazil is considering several proposals regarding cybersecurity, including both unique certification and security requirements for Internet of Things (IoT) devices. In Brazil and other jurisdictions, ITI has a number of questions with regard to whether and how certification should be used as a means of assessing a product against cybersecurity regulatory requirements over the entire

lifecycle of a connected device.[1] 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.

Brazil's August 2018 data protection law and subsequent legislation are currently being implemented, including through the creation of a data protection agency. ITI encourages these processes to be transparent, technical, and in line with global best practices. ITI also urges Brazil to leverage global best practices as it sets up its data protection authority (ANPD) as an independent body and a resource to companies of all sizes that collect, store, and process data in Brazil or with regard to Brazilian citizens. This will be critical for companies that do business in Brazil, and we encourage clarity and predictability for companies that will need to comply with the new rules.

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, Law 8248/91, and Ordinance 87/2013); it offers government procurement preferences for local ICT hardware and software (2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903); 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). In January 2018, the WTO Appellate Body concluded a dispute settlement proceeding brought by the European Union (EU) and Japan surrounding these localization barriers. The decision confirmed several inconsistencies between Brazilian industrial and trade policies and WTO commitments. As Brazil takes steps to bring its policies, programs and procedures in line with its WTO obligations, ITI also encourages USTR to work with the Brazilian government to take the opportunity to create a manufacturing and trade environment that is globally competitive and provides a level playing field for all sectors of the industry.

Brazil's *de minimis* threshold of USD $50 remains applicable only to Consumer to Consumer (C2C) transactions 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

[1] 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

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 2021 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 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 ANATEL and ANCINE question how to regulate these services under existing frameworks, without due consideration of specific market and service characteristics, as well as the technical feasibility of the requirements on these services. 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.

The Brazilian Senate is considering a bill[2] which includes a provision requiring digital platforms to "pay news publishers for use of their content (other than hyperlinks)." Given that U.S. digital platforms services constitute a majority of digital services provided in Brazil, such a requirement would 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.

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 one to five percent (on the basis of global revenue) on revenue generated in connection with three narrowly defined sets of digital services. Other proposals of note would establish a unique COFINS-Digital (contribuição para o financiamento da seguridade social) 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).

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 reaching a multilateral solution to tax challenges arising from the digitalization of the global economy.

Brazil's recently proposed fake news bill (PL 2630) would severely impact the ability of internet

[2] PL 4255/2020 at https://www25.senado.leg.br/web/atividade/materias/-/materia/144233

and other tech companies to do business by putting into place a set of requirements that would prove nearly impossible for internet companies (including email and cloud providers) to comply with, such as those concerning intermediary liability and local presence. The measure would require companies to 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 is expected to pass the Chamber of Deputies with some changes.

ITI urges the U.S. Government to encourage the Brazilian government to implement the Inter-American Telecommunication Commission (CITEL) MRA with respect to the United States. Doing so would allow for recognition of testing done in the U.S., easing the time and cost of exporting to the Brazilian market. ANATEL's Resolution 323 of 2002 is particularly onerous in that it requires producers of telecommunications equipment to test virtually all of their products in country before they can be placed on the market, increasing price and delaying the time it takes for the products to be available to Brazilian consumers.

The Brazil Ministry of Environment National Environmental Council (Conama) is currently preparing to adopt its own Restriction of Hazardous Substances (RoHS) regulation for electronics. This regulation was initially planned to align with the European Union RoHS Directive. However, there are major differences in scope and compliance assurance. ITI sent Conama a detailed list of concerns and urges Brazil to harmonize its regulations with other existing RoHS approaches, rather than creating a distinct national approach.

Brazil took a significant step towards the adoption of good regulatory practices with the publication of Resolution 90 in 2018, which encourages Brazilian regulatory bodies to: develop regulatory agendas; conduct regulatory impact analyses; evaluate regulatory alternatives; base regulatory requirements on international standards; conduct transparent public consultations allowing a minimum of 60 days for public comment for all regulations with international trade effects; ensure all regulations comply with Brazil's international trade commitments; notify technical regulations to the WTO in accordance with Brazil's commitments under existing WTO agreements; use evidence-based decision making; coordinate with other relevant regulators to ensure coherence and compatibility with other regulations; and review and manage regulatory stock.

Despite this positive development, however, a number of consultations notified by ANATEL in 2020 through the WTO TBT inquiry point included very short timeframes for response. We appreciate ANATEL extending the deadlines for comments on a case-by-case basis, but we encourage all agencies in Brazil to notify consultations with a minimum 60-day comment period. Agencies are also encouraged to consider the regulatory impact imposed by requirements and whether the benefits are commensurate with the impacts. For example, the recent operational procedures published for Resolution No. 715 approving regulations for conformity assessment and homologation of telecommunications products contain a number of submission procedures and additional bureaucratic steps that increase burden to industry without providing additional assurance of conformity. In particular:

- The operating procedures contain several bureaucratic processes regarding the submission of information to Designated Certification Bodies (OCD), labs, and ANATEL. In particular, ANATEL's involvement of OCDs in the sample selection, identification, and receipt processes Imposes unnecessary burdens and delays.
- Companies are required to make confidential information available to OCDs and ANATEL, and ANATEL retains the right to publish this confidential information in a public database.
- In terms of market surveillance, we have asked ANATEL to positively consider fair and impartial sample selection processes and testing requirements that are risk-based and include feedback mechanisms. A clearly defined and systematic process for market surveillance, including clarity about the consequences of market surveillance failure are essential.

We encourage ANATEL and other agencies to consider the impacts of regulations in comparison to the benefits provided and to provide an explanation of these benefits in any proposed regulation.

In the past few years, the Brazilian Central Bank's (BCB) role as a regulator and a competitor has created a conflict of interest. The BCB oversees not only the development of policy that affects all payment schemes in the Brazilian market, but also the development and regulation (including participation rules and licenses) of PIX, a real-time payment scheme. In 2020, when U.S. payment networks partnered with WhatsApp and launched a new payments solution to enable WhatsApp users in Brazil to transfer money and pay businesses, the BCB immediately suspended the payments program and abruptly modified the payments regulation (through BCB Circular 4031 dated June 23, 2020), without notice or opportunity for public comment. Additionally, on October 22, the BCB issued a new regulation (Resolution BCB 24) to regulate the activity of payment initiators, a role not previously considered within the BCB's regulatory perimeter. The combination of newly issued regulations, the related requirement for U.S. firms to obtain a new license, and the creation of a new regulated category "payment initiator," is creating a substantial delay for the implementation of the partnership between U.S. payments firms and WhatsApp, which effectively provides PIX with an unfair commercial advantage. We urge USTR to raise concerns on BCB's general adherence to good regulatory practices and the sudden change in the regulation which led to the disruption of the legitimate and licensed supply of a payment solution.

Finally, Brazil is currently reviewing and restructuring its national AI strategy at the federal level, and several bills governing AI have been introduced in the Congress. There is a concern that some policymakers have taken positions on these initiatives that could isolate Brazil through the adoption of unique standards or onerous certification or localization requirements. Industry continues to advocate for the adoption of a flexible and diversified regulatory approach that encourages strong public-private collaboration and responsible development of AI. Further, to promote innovation, we also encourage the facilitation of public data sharing, advancement of structured and standardized AI R&D, and support for STEM-informed workforce development.

Canada

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." It reiterated this message in its most recent annual report.[3] In the meantime, the Government of Quebec has introduced new privacy legislation that, among other things, would make data transfer extraordinarily difficult. ITI is concerned 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. 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 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 commitments under USMCA, which generally prohibits the parties from restricting the flow of personal information between one another (Art. 19.11).

Canadian Prime Minister Justin Trudeau had previously proposed a digital services tax (DST) similar to the French DST. According to a cost analysis conducted by Canada's Office of the Parliamentary Budget Officer, the tax would "replicate" the French measures and impose a 3 percent tax on revenue from advertising services and digital intermediation services for companies that meet certain global and Canadian revenue thresholds. This year's Speech from the Throne reiterated the Canadian government's interest in taxing "digital giants." ITI urges USTR to encourage Canada continue directing its efforts to the OECD project and to refrain from proceeding with consideration of a unilateral DST measure.

The publication of the draft standard ICES-003, Issue 7, "Information Technology Equipment (including Digital Apparatus)" showed a troubling turn towards the non-alignment of standards between the United States and Canada. Despite a stated intent to align Canada's electromagnetic emission requirements with the FCC Part 15 limits, there are two areas of non-alignment: test limits and existing compliant products. To more fully align with the FCC's Part 15 requirements and avoid potential technical barriers to trade between Canada and United States, ITI requested ISED to reconsider the emission limits for Issue 7 to continue permitting compliance with ICES-003 based on meeting either the FCC limits (as defined in Section 15.109 (a) and (b) of the FCC Rules) or CISPR 22 limits. Furthermore, we have asked that ISED allow products already being marketed in Canada (and the United States) prior to the end of the transition period for ICES-003 Issue 7 to continue to comply with the previous Issue of ICES that was used to originally satisfy Canada's legislation applying to interference causing equipment.

[3] https://www.canada.ca/en/privy-council/campaigns/speech-throne/2020/stronger-resilient-canada.html

Chile

Chile regulates the testing and certification for safety for an increasing number of electronics and ICT products. Resolution 16677/2017 and protocol PE-8/8 implemented new requirements that all power adaptors for smartphones be certified by SEC (Chilean Safety Regulator) in Chile and be displayed with the product that contains the charger. This has created challenges and cost increases for companies that have had to adopt the Chile-specific requirement in a short period of time. In 2020, Chile issued the final PE Nº 8/9:2019, which extended the rule to many other power adaptors including those for notebooks, tablets, and audio and video products. ITI urges USTR to encourage the Chilean Government to adopt international standards without adding any Chile-specific requirements, and to accept existing international documentation issued by international bodies under the Scheme of the IECEE for Mutual Recognition of Test Certificates for Electrical Equipment (IECEE CB Scheme).

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

ITI appreciates the work and attention that the U.S. government has dedicated to China and its many discriminatory trade practices. Forced partnerships with Chinese companies, the inability of foreign companies to obtain licenses to operate in China, and data localization 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 2021 NTE and continue to work to implement the commitments of the Phase One agreement and move towards Phase Two.

For example, when China joined the WTO in 2001, it committed to allow non-Chinese 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 looks forward to the processing of RMB-denominated transactions by all U.S. EPS suppliers that have applied for a BCCI license, as contemplated under those agreements.

The Cybersecurity Law (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, especially with respect to the responsibilities and authorities of the Ministry of Public Security vice the Cyberspace Administration of China. These review regimes may compel companies to disclose sensitive information and create an environment conducive to uneven enforcement.

Data localization measures remain in China, though there are signs of the government seeking to identify areas for increased openness through "pilot" foreign trade zones in Shanghai and Beijing geared towards loosening data restrictions that have been problematic for both foreign and domestic companies. Barriers that pre-dated the Cybersecurity Law already cost U.S. service providers billions of dollars as companies were pushed out of the market, with a vast majority of U.S. companies describing Chinese Internet restrictions as either "somewhat negatively" or "negatively" impacting their capacity to do business there.[4] Though there were signs of the Chinese government contemplating lessening restrictions on foreign cloud service providers (CSPs), those prospects have dissipated given increased bilateral tensions. Onerous regulations on U.S. 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. At present, draft and existing Chinese regulations[5] are poised to exacerbate these concerns.

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.

[4] According to ITI member survey conducted in September 2016.

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

Looking beyond cloud services, the most tangible existing data restrictions are found in the *Measures on Cross-Border Data Transfer,* which have remained in draft form since 2017. This summer, China released its draft Data Security Law, which will likely address data transfer requirements more fully in implementing regulations. A critical regulation to watch with respect to implementation is Ministry of Public Security's (MPS) recently released guiding opinion on critical information infrastructure (CII), which will determine whether CII-classified data must remain in China, as prescribed by the CSL.

Also problematic is other nations' mirroring of these policies, without any sense of how to implement them in a significantly smaller and less influential market. Implementation and enforcement of such policies is not realistic, especially in smaller markets – leaving the door open for uneven enforcement targeting foreign companies.

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.[6] 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. Released in September 2020, the draft *Commercial Encryption Administrative Regulations* also imposes a "mass market test" that would unnecessarily regulate any products that have encryption features.

Numerous Chinese standards that are categorized as "voluntary" continue to be regarded by Chinese government agencies as mandatory or *de facto* mandatory. China-unique standards require companies to unnecessarily modify their products or services for China, thus creating a market access barrier to which Chinese companies are not subject. This issue could be ameliorated through more openness of Chinese standards organizations to foreign participants. While the Chinese government has improved foreign company access to Chinese standards development organizations (SDOs), and has vowed to level the playing field in the 2019 Foreign Investment Law, the process still does not allow companies to participate in select bodies that are of greatest interest to them. For example, Chinese SDOs often require that participants attend – and vote during – every meeting. Without substantial human resources, including technical expertise and the ability to read Chinese fluently, most foreign companies can simply not keep pace and subsequently find themselves excluded. We encourage USTR to press the Chinese government to ensure that practices like these are addressed as part of China's implementation of the Foreign Investment Act. We encourage the U.S. government to work with other nations to discourage China from creating unique standards and instead rely on – and continue to participate in the formulation of – *voluntary* international standards. However, it

[6] 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.

should be noted that recent U.S. policies, such as Department of Commerce restrictions on standards development activities related to the Huawei entity list designation, have led certain international and U.S. SDOs to conclude that they cannot allow certain Chinese companies to participate without violating U.S. export controls. This unintended consequence has not only made U.S. companies less competitive but it has also made it increasingly difficult to advocate for increased openness of Chinese SDOs and alignment of Chinese standards with those produced by such international organizations.

Colombia

Colombia has not implemented the $200 *de minimis* threshold on duties or taxes commitment provided for in the U.S.-Colombia Trade Promotion Agreement (CTPA). On July 2, 2019, the Colombian government published Decree 1165 of 2019, which established Colombia's New Customs Regime. The new regime combined all relevant decrees and regulations issued over the last few years and by doing so, scrapped Decree 349, and removed any specific timeline to implement the *de minimis* provision of the CTPA. In addition, Colombia has also significantly delayed implementation of customs reforms that would allow traders to submit electronic copies of invoices instead of physical copies.

The Superintendency of Industry and Commerce, the consumer protection authority in Colombia, undertook efforts in 2019 to amend its "Circular Única" requiring all mobile phone manufacturers and retailers to include a specific label indicating the device's compatibility with all mobile networks (e.g. 2G, 3G, 4G and 5G). The label is required for all phones, even those that operate in all bands. If enacted, this labelling system will create challenges and increase costs for companies that must adopt the Colombia-specific requirement, thereby increasing consumer costs. ITI urges USTR to encourage the Colombian Government to revise its proposal and avoid the creation of these country-specific label requirements, as they will prove an ineffective way to alert the Colombian consumer about a smartphone's functionalities. We encourage cooperation between agencies like SIC, and the trade ministry (MinCIT) so that regulatory can fully understand the trade impacts of their measures.

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.

Egypt

In July 2020, Egypt enacted its first general privacy legislation, the Data Protection Law. The Law imposes significant administrative and regulatory burdens on all entities operating in Egypt, with no exemptions on the basis of an organisation's size. The Law is due to come into full effect following the passing of Executive Regulations, expected in or before April 2021.

Key components of the Data Protection Law include:

- Sensitive Personal Data, including financial data, requires explicit consent to process (exemption for entities under Central Bank supervision)
- Accountability, including DPO appointment requirement and data breach notification obligations
- Records of Processing required
- Grounds for processing and cross-border data transfers are limited
- Restrictions on re-use of data by organizations
- Licenses are required for several activities

European Union

A new European Commission took office in May 2019 and has since pursued an active digital policy strategy under the banner of "technological sovereignty", which is geared towards boosting the capacity of Europe's domestic technology industry and may affect the conditions under which non-European firms can compete in the European single market. Under a new, sweeping Digital Services Act the EU is proposing new *ex ante* regulatory rules that may affect various aspects of U.S. platforms' business models. Other initiatives, described in more detail below, center on data governance, artificial intelligence, and cloud services. Maintaining and increasing the ability to develop key technologies and ensure their availability to the EU in the future is a legitimate goal, and ITI strongly supports the pursuit of these 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 Europe's vision of technological sovereignty, which remains a vague concept. Relevant policy processes currently in motion include but are not limited to:

- **The Digital Services Act** (DSA)**,** for which a legislative proposal is expected in December 2020. The DSA will seek to update the legislative framework for online platforms currently governed by the E-Commerce Directive of 2001. In addition to revisiting the liability regime for online platforms, the new legislative package will likely address gatekeeper effects of large platforms. In parallel, the Commission has launched plans to work on a New Competition Tool that would allow the Commission to exercise its antitrust powers in (digital) markets where it deems competition is at risk of distortion, including against non-dominant companies and absent an actual infringement of competition rules.
- **The European Data Strategy,** which contemplates several legislative initiatives that will affect all players in the tech industry as well as other industrial sectors through increased data sharing provisions between public authorities and private firms to create a "European data space." A data governance proposal due in November 2020 and a Data Act due Q1 2021 could introduce mandatory data sharing obligations for companies that could have significant disruptive effects on industries.
- **Artificial Intelligence** regulation, with a legislative proposal expected in Q1 2021. Based on the February 2020 European Commission White Paper, the Commission has advanced

a stated goal of building an ecosystem that can support the development and uptake of AI across the EU economy and public administration. The paper considers, among other options, the possible reliance on the EU's existing *ex ante* conformity assessment infrastructure to audit high-risk AI applications, giving EU regulators and testing entities (i.e., Notified Bodies) potential authority to audit and delay introductions of certain AI applications to the EU market. Consultations conducted since the publication of the White Paper also contemplate the introduction of labeling requirements, transparency and reporting obligations, and requirements to train AI systems on European data. Such requirements, and in particular *ex ante* testing requirements and the potential requirement to train AI algorithms using European data, may create barriers to entry for non-EU AI services.

- 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 remains unclear and could create technical barriers to trade as well as barriers to services trade. This is particularly the case if these requirements are not based on existing international standards and testing to such requirements does not allow for market participation of non-EU testing bodies. ITI continues to advocate for global, industry-driven, voluntary-consensus standards to serve as the basis for all future schemes.
- The establishment of a unified European cloud and data ecosystem (**GAIA-X**) and European cloud federation, under which we understand efforts are underway to develop "codes of conduct" and other approaches that might be potentially restrictive and discourage reliance on international standards. While developments are still in flux, reliance on these codes or other technical specifications that are not aligned with global, industry-driven, voluntary consensus standards may limit the ability of foreign cloud service providers from engaging in the European market, and in public tenders in particular.
- The potential introduction of a new EU-wide **digital services tax measure**. The Commission has reiterated its intent to – in the absence of satisfactory political agreement as part of ongoing negotiations at the Organization for Economic Co-operation and Development (OECD) – introduce an EU-wide digital tax in the first half of 2021. Members of European Parliament have also voted to pass a budget that includes revenue from a digital tax starting in 2023. We remain deeply concerned with the prospect of an EU-wide digital tax proposal and the enactment of unilateral, digital services taxes (DST) by Austria, France, Italy, Poland, and Spain, as well as the introduction of DST measures by four other individual EU Member States. As outlined in detail in ITI's submission in response to USTR's Initiation of Section 301 Investigations of Digital Services Taxes,[7] the

[7] Submission available at: https://www.itic.org/policy/2020.07.15ITIFinalSubmissionDSTInvestigations.pdf

measures identified in the 2020 Section 301 investigations replicate many design elements of the French DST, which USTR has found to be discriminatory and burdensome to U.S. commerce. Additionally, comments by relevant senior officials have echoed those by French senior officials prior to and following the enactment of the French measure to strongly suggest that the measures are discriminatory in nature. We encourage USTR to continue to use the 2021 NTE to raise the significant trade-related concerns posed by all unilateral digital services taxation measures, including those put forward to date in Austria, Belgium, Czechia, France, Hungary, Italy, Poland, Slovenia, and Spain.

Many of these workstreams are at relatively early stages in their respective legislative processes. Industry will continue to actively engage in the development of these policies with a view to mitigating the introduction of trade-restrictive measures, including 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 support the establishment of a structured bilateral dialogue between the United States and 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 recently 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 standard contractual clauses (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. The most significant concerns remain around surveillance practices of the U.S. government and whether EU citizens' data would sufficiently be protected from law enforcement access by U.S. authorities. ITI continues to recommend a meaningful political resolution through ongoing negotiations between the Department of Commerce and the European Commission to help ensure that transatlantic data flows and transatlantic trade can continue with as little interruption possible.

On September 4, the European Data Protection Board (EDPB) created a taskforce to look into complaints filed in the aftermath of the CJEU Schrems II judgment, and the group is expected to publish guidance for controllers/processors on international data transfers in coming months. The timing will be linked to the European Commission's parallel work on a new set of SCCs expected before the end of the year. ITI is committed to supporting EU and U.S. policymakers in working towards a successor agreement to Privacy Shield. In this context, ITI welcomed in particular the Commerce Department's statement on the Schrems II case ruling and the SCCs joint white paper with the Department of Justice and Office of the Director of National Intelligence, providing guidance to companies impacted by the ruling.

In addition to horizontal policy efforts, the European Commission has also proposed regulating aspects of new technologies through revisions to existing vertical legislation. The Commission continues to assess the need to revise existing legislation such as the Product Liability Directive, the General Product Safety Directive, and the Machinery Directive. These laws are seen as having potential gaps with respect to the regulation of innovative technologies, although it is important that a potential revision of these existing laws maintain coherence alongside parallel new initiatives on, e.g., AI. 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.

In the same vein, the Commission is also assessing possible updates to the Radio Equipment Directive (RED) that could create technical barriers to trade. One such update would potentially generate new security and privacy requirements for wearable devices. The compatibility of such requirements with existing and forthcoming requirements under the GDPR and the EU Cybersecurity Act, respectively, remains a key question for industry. Another delegated act under the RED would ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated. ITI is concerned by the development of isolated new regulatory requirements within vertical European legislative acts, such as the RED, to address what are fundamentally horizontal issues. As with the Machinery Directive, 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.

A separate Commission initiative under the RED developed an impact assessment regarding a common charger for mobile devices. In September 2020, it was announced that the Commission will undertake two studies related to common charger under RED, one on decoupling and the other on wireless charging. ITI strongly urges the Commission to avoid any regulatory approach mandating the uptake of a prescriptive common charger solution, which would undo the current market progression towards increasing common charging interoperability across a range of mobile products while supporting industry innovation, and create potential technical barriers to trade.

As concerns more systemic challenges to ICT regulatory compliance, we also wish to flag issues related to the European standardization system and the New Legislative Framework (NLF). Across harmonized European product legislation (so-called New Approach legislation), European harmonized standards (hENs) are accorded a "presumption of conformity" under EU law that provides relative certainty that products built to such hENs will be deemed compliant under relevant harmonized legislative acts. While firms may technically still produce to non-hENs, the pathway for demonstrating compliance when doing so is more burdensome and involves assessment by a designated, EU-based conformity assessment body (a "Notified Body"). For ICT product safety, hENs are often based on existing international standards (e.g., IEC standards). However, we are alarmed by the recent trend whereby European standards sometimes diverge from standards developed by international SDOs, which are vetted and voted on by international technical experts, including European experts. These divergences between hENs and widely adopted international standards, which are often preceded by lengthy delays in adoption process, are due to, among other factors, the particularities of the updated Harmonised Standards (HAS) Consultant system.

Although the review of hENs is intended to ensure their alignment with corresponding European essential requirements, the resulting inefficiencies, reflected in part in the intervention of HAS consultants, are having a detrimental impact on the ability of industry and stakeholders to rely on harmonized standards to place products on the Single Market. Implementation of these checks on standards has inadvertently slowed the process of European standards development, which hampers the ability of the current system to keep pace with technological developments. Specifically, the HAS consultants process has raised challenges to fundamental technical and physical principles against the consensus positions of the international technical expert community, often at the end of the standards development process rather than during, thus delaying adoption of harmonized standards. Industry has also often observed cases where there are diverging views expressed by the Commission desk officers at the very end of the approval process, thus either delaying or blocking the citation of the European harmonized standards in the Official Journal of the European Union (OJEU).

A further, emerging industry concern is the development of technical specifications or "codes of conduct" through ill-defined processes outside of the NLF framework. In recent engagements with the Commission and USTR, ITI has raised concerns about what appears to be an increasing reliance by the Commission on such "codes of conduct" or technical specifications, rather than hENs as prescribed by the NLF, as a means of informing potential mandatory requirements in specific areas of innovative technology. Adding to industry concerns is the lack of due process or clear terms of open participation in the development of such specifications. Industry has noted the increasing prevalence of such relatively closed processes in relation to data portability specifications under the Switching Cloud Providers and Porting Data (SWIPO) multi-stakeholder group, the development of GDPR certification requirements, the work of *ad hoc* groups established in relation to specific schemes in development under the Cybersecurity Act, and, as noted above, in the context of GAIA-X. The potential for increased reliance on the products of these closed processes, rather than international and/or hENs, presents serious concerns for

industry, and we encourage U.S. engagement to ensure that such processes do not lead to unnecessary, fragmented requirements.

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.

In July 2018 the European Commission notified a Draft Regulation Implementing Directive 2009/125/EC regarding eco-design requirements for servers and data storage products (referred to as "Lot 9"), to the World Trade Organization (WTO) Technical Barriers to Trade (TBT) Inquiry Point. The regulation does not fully align with imminent international standards (ISO/IEC 21836) and includes ambiguous and potentially unnecessarily burdensome conformity assessment methods. This failure to align with international norms and best practices creates technical barriers to trade. Further, presenting a draft regulation to the European Parliament and Council that significantly deviates from the version of the regulation notified to the WTO creates business uncertainty and contravenes the EU's notification obligations. ITI is still awaiting a response to the FAQ industry has sent it regarding four key issues left from the adopted Servers and Data Storage Products Regulation: conformity assessment; clarity on network switches, the ability to charge a commercially reasonable price for firmware, and flexibility in being able to disassemble components.

In December 2017, the European Commission initiated a two-part legislative proposal (the Goods

Package) aimed at improving product safety across the EU: (1) a draft regulation on compliance and enforcement (market surveillance); and (2) a draft regulation on mutual recognition for the EU Single Market. The Commission notified the package to the WTO in February 2018. The final Regulation (EU) 2019/1020 on market surveillance and product compliance entered into law on July 15, 2019 with the majority of its provisions applicable as of July 16, 2021. The Regulation includes a number of ambiguities that may prejudice legitimate traders seeking to access the EU market, while doing little to improve overall customer safety. Specifically, Article 4 includes a requirement for a dedicated "Responsible Person" who must be based in the EU and who will be responsible for maintaining compliance documentation and cooperating with market surveillance authorities to furnish that information, as necessary (for a limited range of product categories). Article 4 lacks clarity, however, regarding the responsibilities and liabilities for the Responsible Person, including fulfilment service providers, by taking a one-size-fits-all approach to liability regardless of objective and risk. Final guidance is expected to provide clear advice and mechanisms to businesses who want to comply, and to ensure implementation of the Regulation is consistent with the EU's obligations under the WTO TBT Agreement. It is worth noting that the EU is currently reviewing the 2001 General Product Safety Directive and is looking at the Article 4 provisions and whether these would apply to all products, an outcome that would be disproportionate and further act as a barrier to legitimate traders.

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.

The European Commission has proposed new powers to investigate and sanction foreign subsidies that have allegedly distortive effects on the EU's internal market. The proposals would enable the Commission or Member States to challenge distortive foreign subsidies (including acquisitions and public procurement) and provide rectification powers if distortions are found (module 1). It would also require notifications of acquisitions that could be facilitated by foreign subsidies and would allow the Commission to impose remedies or block the acquisition (module 2). Finally, it would establish a notification obligation for potentially subsidized bids and allow the potential disqualification of the bidder from public procurement procedures (module 3). Foreign subsidies would be broadly defined as any financial contribution or benefit from a non-EU state. These proposals could empower the Commission to rely on alleged foreign tax advantages to scrutinize any private company's activities and acquisitions in the EU. Each module follows four steps: (i) determination of whether a foreign subsidy is involved; (ii) the identification of market distortion caused by the foreign subsidy; (iii) an EU interest test balancing positive effects, based on EU political priorities, against distortion; and (iv) imposition of remedies as determined by the EC. The contemplated remedies that could be imposed on companies found to have received

distortive foreign subsidies are broad. They could include investment bans, divestment of assets, third party access rights (e.g., to data or IP), conduct requirements, or prohibition of certain conduct.

Lastly, we would like to voice our support for the retention of the EU Customs Barriers and Trade Facilitation language from the 2020 NTE Report in the 2021 NTE Report. In addition to EU-wide policies addressed above, we wish to call USTR's attention to several Member State-specific initiatives.

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. According to the communication, in-scope companies would be subject to precautionary measures to maintain in Finland information systems and information resources deemed necessary for the uninterrupted operation of the financial markets. In July 2020, in order to assess any gaps in preparedness capacity, 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 will then inform the work of the Ministry of Finance, which intends to issue legislation in 2021. Industry is concerned that such legislation could impose an indirect data localization requirement, presenting potential market access barriers and distorting competition in Finland for CSPs that do not have local data centers.

France

Some industry stakeholders have noted that the French cyber-security agency (ANSSI) is currently blocking applications to enter into the qualification process for its *SecNumCloud* security certification due to concerns around the U.S. CLOUD Act and the purported need for the localization of certain services. Receiving the certification is an important validation for the cloud-to-commercial sector. We respectfully request U.S. Government engagement to raise concerns with the Prime Minister and the Ministry of Foreign Affairs that *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.

Sweden

U.S. cloud service providers (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.

India

India's digital ecosystem has significantly degraded for American companies over the past several years. ITI is increasingly concerned with India's restrictive data policies which have and will continue to generate unnecessary trade barriers for U.S. companies. We recommend that USTR continue its robust engagement on these issues, both by highlighting them in the 2021 NTE as well as through direct bilateral and multilateral engagement discussion in every available forum.

In December 2019, the Government of India (GOI) submitted its long-awaited privacy legislation to Parliament, the Personal Data Protection Bill (PDPB). If enacted, the PDPB would prohibit 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. In addition, the PDPB provides the GOI with a new, broad authority to request non-personal data from companies with very little discussion of how such a request would work in practice or whether industry would have recourse to legal protections or due process. The Bill contains many remaining issues that create uncertainty and new regulatory burdens for companies without improving the privacy of Indian citizens. 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 their otherwise limit their operating space within India. We request that the 2021 NTE highlight the trade-restrictive elements of the PDPB.

In February 2019, the Department for Promotion of Industry and Internal Trade (DPIIT) released the draft National E-Commerce Policy, which, among many other troubling elements, contained

requirements to share data, broad forced data localization and restrictions of cross-border data flows, additional liabilities on intermediaries, and a rejection of the WTO Moratorium on Customs Duties on Electronic Transmissions and the WTO E-Commerce Negotiations. The release of an updated draft of the policy appears to be imminent and we expect that it will retain many of the problematic elements that the initial draft contained.

On July 12, the Indian Expert Committee constituted by the Ministry of Electronics and Information Technology (MEITY) to deliberate on a Non-Personal Data (NPD) Governance Framework released its long-awaited Report for consultation. If adopted by GOI, the recommendations in the report would have a significant, negative impact on most if not all companies that do business in India. The regulation of NPD would constitute a significant divergence from global privacy best practices and would set a negative precedent for digital policies worldwide. The Report's recommendations outline a new framework to enable – and, in many instances, require – the sharing of data held primarily by multinational companies with companies in India and the GOI. It seeks to achieve this aim by defining types of NPD (including a novel category called "community data"), establishing acceptable purposes under which third parties can request access to privately held NPD, and creating roles and responsibilities for different actors in the NPD ecosystem. The Report also recommends creating a new Non-Personal Data Authority (NPDA) that would oversee and enforce the proposed obligations, which include new company registration requirements and mechanisms through which companies or the GOI can request access to data.

Some of the more concerning recommendations of Report include: requiring private entities to share not only raw data they collect, but also insights derived from such data, and data collected outside India with no nexus to India; overly broad bases for requesting sharing of data, effectively requiring private entities to share their data with anyone who requests it; requiring that the sharing by private entities of data be without charge, unless the data has undergone sufficient (but undefined thresholds of) value-added processing; and giving third parties beneficial ownership/interests over private entities' data, where such data is considered to be "community non-personal data." We request that USTR highlight this report in the 2021 NTE and continue to aggressively oppose its adoption by the GOI.

The Indian government's think tank, the NITI Aayog, released a draft policy document – the "Data Empowerment and Protection Architecture" (DEPA) in September 2020. The DEPA is a consent-based framework for individuals to securely access and share their information between businesses. By proposing a new technological architecture consisting of India-specific data protection, processing, and sharing standards, the DEPA could lead to trade-restrictive standards that impose unnecessary burdens on foreign companies.

In August 2018, the Ministry of Health and Family Welfare (MoHFW) released a draft set of amendments to the Drugs and Cosmetics Rules (1945) to regulate online pharmacies in India. Proposed Article 67.k(3) mandates that the e-pharmacy portal shall be established in India and that it shall keep the data generated localized. It further prohibits the transfer or storage of data generated or mirrored through the e-pharmacy portal outside of India. While a final version of

the rules have not yet been released, if enacted, this policy would discriminate against foreign firms by raising barriers to entry and operation, given that many foreign companies leverage global storage systems for optimizing service delivery by default.

In December 2018, MeitY proposed Intermediary Liability Guidelines that outline safe harbor protections for intermediaries in India and impose significant and burdensome requirements on companies that fall within scope. While these requirements would apply equally to local intermediaries, foreign intermediaries have an additional obligation to set up a separate registered Indian presence and entity, and to appoint a local nodal officer and grievance redressal officer. These requirements disadvantage foreign intermediaries that otherwise may not have a local presence.

MeitY regulations require that Cloud Service Providers (CSPs) who wish to be empaneled to bid for government contracts maintain data centers at least 100km apart. The Securities and Exchange Board of India (SEBI) has similar requirements (the request is for data centers is to be at least 500 km apart). The Insurance Regulatory and Development Authority of India (IRDAI) and the Reserve Bank of India (RBI) do not appear to have any over-riding policy statements, but are known to advise banks and insurance companies to follow a similar mandate. These pose significant burdens to U.S. companies' operations in India, especially for many U.S. CSPs who are unable to comply with these cumbersome requirements.

Released in 2015, the Department of Electronics and Information Technology (DeitY; now known as MeitY), issued Cloud Computing Empanelment Guidelines for CSPs to be provisionally accredited as eligible CSPs for government procurement of cloud services. Within these Guidelines, Article 2.1(d) requires CSPs to store all data in India to qualify for this accreditation. This Article can be fulfilled by-default by Indian CSPs, whereas non-resident CSPs have to modify their services to be eligible for consideration.

Further, CSPs face significant regulatory challenges in operating and managing data centers in India. These challenges include an inability to buy dark fiber in order to construct and configure their networks, a prohibition on the purchase of dual-use equipment used to manage and run those networks, an inability to own and manage a network to cross-connect data centers and connect directly to an Internet Exchange Point (IXP), and high submarine cable landing station charges. These restrictions significantly impact the ability of U.S. CSPs to configure and manage their networks to optimize access by customers, minimize latency and downtime by choosing ideal routing options, and reduce the capex and opex costs incurred in offering cloud services in India. Compounding concerns around India's cloud ecosystem, the Telecom Regulatory Authority of India (TRAI) released recommendations that would provide the Department of Telecommunications the authority to create a new, non-profit industry body comprised of the compulsory membership of all CSPs to regulate cloud services despite near-unanimous industry opposition. The reason to have such a body is unclear, as is the scope of what it is meant to regulate, creating significant uncertainty in an industry that is already overly burdened by regulation in India.

The National Payment Council of India (NPCI) is a quasi-government agency that operates the largest domestic payment system in the country, including United Payments Interface (UPI) and RuPay (debit and credit) cards. In the past several years, the GOI has taken many direct and indirect actions that give preferential treatment to NPCI, some of which are enumerated below and give an unfair advantage to NPCI, creating a non-level playing field for U.S. EPS providers.

In April 2018, the Reserve Bank of India (RBI) issued a directive for payments firms to store data solely in India and ensure that any data processed abroad be deleted within 24 hours. The payment networks have complied with the RBI directive after investing significant capital and despite the short deadlines. In a recent development, the RBI, in a submission to the Joint Parliamentary Committee overseeing the PDPB, requested that financial data not to be classified as Sensitive Personal Data; however, it also requested that RBI be exempted from the PDPB, which could further set the stage for full on-soil data processing and/or access requirements.

In August 2018, the Finance Ministry's Department of Financial Services issued a circular requiring any re-carding or issuance of new cards by banks to be compliant with the standards defined for the National Common Mobility Card (NCMC). Subsequently, the Ministry of Housing and Urban Affairs (MoHUA) mandated that NPCI qSPARC standards would be the NCMC standards. In late 2019, payment networks agreed to comply with these standards but they have still not been made available or published. This not only creates a non-level playing field for international networks, but also hinders the regular issuance of foreign network-issued cards. Rupay and NPCI are the de facto solutions for any Government disbursement programs, known collectively as Direct Benefit Transfers (DBT) and are now being aggressively pushed into the Government driven credit and commercial transactions, keeping the international networks out of consideration.

Storage of card on file and tokenization are globally recognized to offer faster more secure and seamless customer experiences where B2C or Account to Account transactions are concerned. In September 2020, the RBI issued guidelines disallowing storage of Card on File by merchants and payment aggregators. However, as this ban did not extend to the UPI network, it provides NPCI an unfair advantage.

A January 2020 circular from the RBI mandated that effective October 1, 2020, all cards that would be reissued would need to be switched off for e-commerce, contactless, and international usage, effectively targeting international networks, as RuPay has minimal international acceptance and very limited number of contactless cards in circulation.

Effective April 2020, the Government of India expanded its existing Equalization Levy (EL) to include a 2 percent tax on the sale of goods and services to Indian residents by non-Indian e-commerce companies. The design of this levy explicitly excludes Indian e-commerce 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

incorporation of the levy into the Finance Act, 2020 at a late stage – without any Parliamentary discussion or public consultation – combined with an effective date just four days after passage and a lack of sufficient guidance have also led to significant compliance challenges. ITI 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.

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 international safety requirements in India despite having already passed identical 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, the MeitY proposed to expand 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 certain other countries, rather than on product safety and risk to the Indian public.

Adequate transition times also continue to be a challenge for industry seeking to comply with CRO. Phase IV of CRO was announced on April 22, 2020 with an effective date of October 1, 2020. This timeline was incredibly ambitious, and at industry's request, MeitY ultimately extended the effective date to April 1, 2021. Although industry appreciates the extension, we have asked the GOI to consider as a standard practice setting the effective date 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 2021 NTE and in direct engagement with Indian trade officials.

In May 2017, India's Telecommunications Engineering Centre (TEC) proposed Mandatory Testing & Certification of Telecom Equipment (MTCTE) for all telecom products regulated under India's Telegraph Rules. These changes include 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. TEC and the Department of Telecommunications (DoT) have not provided a rationale or details on the implementation of this broad certification framework, nor have they notified it to the WTO TBT Committee. Many of these requirements will likely be redundant with existing international testing and certification of telecom products. Moreover, India lacks sufficient capacity and infrastructure to implement these changes. Adding to industry uncertainty, the requirements were set to begin in October 2018, but the date has consistently slipped and the online portal for submissions is not active. To avoid a scenario like the CRO, as well as potential overlap with CRO, ITI and local industry are asking TEC/DoT to pare back the initial scope of the MTCTE requirements and clarify a range of outstanding issues. We are also urging the authorities to follow global best practices and accept

international test reports and certificates when applicable, and to allow for additional consultation with industry and an adequate transition time. We request support from the U.S. government in this process.

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, and again in October of 2018. Indian officials have 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. 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 2021 NTE, in bilateral discussions, in WTO committees, and potentially through WTO dispute settlement.

In December of 2018, MEITY notified new amendments to the Information Technology (Intermediaries Guidelines) Rules, 2011. These amendments could contain a number of troubling elements and requirements for online service providers, including proactive monitoring requirements, requirements to be able to trace users, local presence requirements, and short response timelines. The government has yet to come out with its long-awaited update to the initial draft, though we expect that they will continue to contain many of the troubling elements listed above. We recommend that USTR engage directly with the GOI on this issue and monitor closely as the new requirements could significantly impact the ability of American online services to do business in India.

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 for ICT Articles than through SDSs.

Another concern for the tech sector is the treatment of plastic waste. India does not have a single federal mandate, but instead each state has its own independent rules, which leads to

inconsistencies and high costs for industry. Industry urges that India find a way to ensure consistency in its plastic waste rules across the country. We further recommend that India ensure that its rules are consistent with treatment of plastic waste in other major economies.

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 2021 NTE to push the government of India 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.

Indonesia

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") has been 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.

In May 2019, Bank Indonesia 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 indicates that BI will be reviewing existing payments regulation with a view to creating an umbrella payments regulation. BI should ensure consultation with the private sector (both foreign and domestic) during this process.

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 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. The National Payment Gateway regulation, which caps foreign ownership at 20 percent, effectively requires U.S. companies to relinquish control over ownership, pricing, branding, and rules to local entities.

BI released the Payment Transaction Processing regulation (PBI 18/40/2016) in November 2016. This regulation introduces licensing requirements for e-wallets and payment gateways. This regulation also requires all domestic transactions to be processed domestically and introduces a foreign equity cap of 20% on all payment system providers. Existing payment system providers do not have to meet this local ownership requirement provided they do not change equity structure or apply for any new license.

The National Payment Gateway (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% 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 4 domestic switches (Artajasa, Rintis, ALTO, Jalin) and the 4 largest banks (BCA, Mandiri, BRI and BNI).

On September 20, 2017, Bank Indonesia (BI) released implementing guidelines (PADG 19/10/2017) for the National Payment Gateway (NPG) regulation (PBI 19/8/2017) along with three appendices (including pricing guidelines which sets 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 2 out of 4 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.

On May 7, 2018 Bank Indonesia issued a new regulation on e-money (PBI 20/06/2018). The regulation defines e-money as closed-loop or open-loop, server-based or chip-based, and unregistered or registered. The regulation requires non-bank electronic money issuers to have at least 51% local Indonesian ownership. To become a principal/switch, payment service provider must follow two requirements: (i) maximum 20% foreign equity cap as defined in BI regulation no 18/40/PBI/2016, and (ii) on-soil processing capability as defined in BI regulation no

19/08/PBI/2017 on NPG. The regulation also states that a payment system operator cannot control both back end (defined as principal, switching, clearing and settlement) and front end (defined as issuer, acquirer, payment gateway, e-money issuer, and fund transfer operator). The regulation requires all e-money providers to route transactions over the NPG (including cross-border).

BI regulation no 21/18/PADG/2019 requires Indonesia's Standards of QR code (QRIS) for payment be used for all QR domestic as well for inbound cross-border. The regulation also specifies parties involved in QRIS transaction: 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 first step before requesting BI approval. This creates a burdensome approval process. For the in-bound cross-border, the regulation only allows issuing and/or acquiring Banks in Category IV to establish partnership to enable foreign-managed sources of funds and/or foreign-issued payment instruments. As existing local QR code payment providers are making their adjustments to adopt QRIS by latest December 31, 2019, BI has indicated it will set the MDR of 70 bps per transaction.

Looking beyond the payments sector, we are cautious of potential discriminatory treatment of U.S. firms as Indonesia seeks to develop cybersecurity policies and pass its Personal Data Protection bill. Indonesia's government is drafting a Cybersecurity Law which provides for the possibility of certification schemes that may discriminate against foreign firms operating in Indonesia. The draft Personal Data Protection bill is modelled after the EU GDPR and limits cross-border data transfer 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 countries. We encourage the U.S. government to continue to engage Indonesia on its cybersecurity and data protection policies to ensure that implementation does not create barriers to trade.

Indonesia's Ministry of Finance 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 December 2019. While the tariff rates remain at zero, Indonesia's actions have established a dangerous precedent and will likely have the effect of encouraging other countries to violate the WTO Moratorium. 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) entered into force on November 25, 2019, after having been issued and signed without a transparent opportunity for stakeholders to review and provide comments. The regulation provides 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 it has over 1,000 domestic transactions annually), promote domestic products on their platform, and share corporate statistical data to 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 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.

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 is detrimental to the ease of doing business.

In 2019, two regulations were released by KOMINFO: No. 9 of 2019 (Wavelength Division Multiplexing) and No. 10 of 2019 (Internet Protocol Networks), both of which 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, "Provisions and Procedures for Calculating the Value of Domestic Component Levels of Electronic and Telematics Products." Even with the issuance of Regulation No. 22, industry is still in the process of determining how, in practical terms, to comply with the parameters it establishes. We anticipate that U.S. companies will face significant additional compliance costs in order to meet these levels, which are likely to have significant impacts on global supply chains.

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 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. The most recent example of this is the regulation on wavelength division multiplexing (No. 9, cited above), which was released to the public in October 2019, but had been signed on September 5 and entered into force on September 12. This type of retroactive applicability of regulations makes compliance by industry extremely difficult and costly. ITIrequested 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. Several of these issues have been communicated to the SDPPI via letters from ITI and inclusion in the 2020 NTE. However, given the lack of response and engagement from the Indonesian government, continued bilateral prioritization and inclusion of the issues in the 2021 NTE will further emphasize their importance.

The *Draft Regulation Regarding the Provision of Application and/or Content Services Through the Internet,* first opened for comments in May of 2016, places vague requirements on providers of OTT services. The most onerous requirement is that OTT services must "place a part of its servers at data centers within the territory of the Republic of Indonesia." It is not clear what "part of its servers" means precisely, nor is it clear why this requirement is in the draft regulation—there seems to be a line of rationality drawn between this draft regulation needing to mirror Regulation 82/2012. This law has the potential to cause serious damage U.S. business interests in Indonesia by requiring a level of local presence that is neither beneficial nor necessary. Furthermore, the regulation would impose significant responsibilities on OTT service providers, such as content monitoring and handling that is often beyond their control.

On March 31, the Government of Indonesia adopted several digital tax measures through an emergency administrative decree. 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. Though the Government has not yet published implementing regulations, the ETT legislation creates 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. We understand that USTR has started a Section 301 investigation into Indonesia's ETT.

Indonesia currently imposes restrictions on foreign direct investment 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% 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

Japan has established a new regulation on "platform-to-business" (P2B) relations that would require online intermediaries to meet aggressive transparency obligations concerning differentiated treatment and access to data. These rules will be 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 law is set to enter into force by April 2021.

Kenya

Kenya's Finance Bill, 2020 established a 1.5 percent tax on gross transaction value for services sold through a digital marketplace. The tax will be offset by income tax paid by resident and nonresident firms, thereby effectively limiting exposure to nonresident firms. Draft Income Tax (Digital Service Tax) Regulations, 2020 were released in July, and the measure is effective January 1, 2021. ITI urges USTR to encourage Kenya to refrain from implementing the digital service tax and instead re-commit to the multilateral project through the Inclusive Framework to address tax challenges of the digitalizing global economy.

Kenya's Data Protection Law, which was adopted in 2019, 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.

Kenya's 2020 National ICT Policy Guidelines require that Kenyan data collected by the government for the purpose of providing public services "remains in Kenya."[8] The Data Protection Act[9] which was passed in 2019 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. Kenya's new ICT Policy also includes a clause on "equity

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

participation." The policy increases local ownership rules from 20% to 30%, although the requirement is not set to come into effect for three years. If these provisions are enacted, only firms with 30% "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 (as-of-yet unformed) Office of the Data Commissioner, but it does set a direction of travel for those agencies.

Malaysia

In December of 2016, the Malaysian Communications and Multimedia Commission (MCMC) announced that it would introduce a mandatory type approval and certification to IPv6 Technical Code, MCMC MTSFB TC T013:2016 in accordance with the Communications and Multimedia Act 1998. While some countries regulate for IPv6, nearly all either only apply such requirements to government procurement or purchases in the B2B market. Malaysia initially applied the requirements to a wide range of products and unjustifiably bundled them with those for safety and EMC. Following repeated engagement with MCMC to seek a reduction of product scope for this program, MCMC relaxed certain requirements. In August of 2019, MCMC announced modified Technical Code, MCMC MTSFB TC T013:2019 and stated that it would enforce IPv6 certification from July of 2020. Despite improvements in the modified Technical Code, as concerns the certification of hardware, Safety and EMC requirements remain. Industry also has yet to see an official process document yet for certification operations, and respectfully requests that USTR continue to monitor the implementation of the technical code to ensure it does not generate 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, and ITI understands that the program may be broadened in the beginning of 2020. Developments in this area seem to have been placed on hold. 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.

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 GATS commitments. However, payment providers have to obtain approval from BNM, which is subject to meeting conditions such as safeguards to protect and access data located offshore, enabling interoperability and reducing fragmentation of multiple providers and pricing transparency.

Mexico

ITI has been tracking a number of legislative proposals in Mexico targeting OTT services. The Mexican Senate is considering a measure that would introduce local content quotas of 30% for music or video streaming services, as well as impose a new registration requirement with the telecommunications authority, IFT. As a result of this registration, OTT services would be regulated under the Federal Telecommunications and Broadcasting Law and likely forced to comply with its mandates for restricted audio/video services. These requirements would create a significant barriers to the operations of ITI members in Mexico and raises questions under Mexico's trade obligations, in particular its commitments in the telecommunications chapter of USMCA.

On September 8, 2020, 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," which is 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. While the government ultimately removed the measure from last year's budget proposal, the fact that a limited number of companies registered in the government's regime (35 companies in Mexico, compared to more than 100 in Chile in the same timeframe, due to Mexico's incredibly complex registration process) has led it to reintroduce the measure as way to force compliance. Should the regime be approved, 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.

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 NOM-029 deviates from this regionally and internationally accepted practice and imposes significant burdens on industry.

On April 20, 2015, the Mexican tax authority (SAT) issued an amended version of the Customs Law Rules (*reglamento de la ley aduanera*), ostensibly to harmonize its terminology and regulatory definitions with the Customs Law while including new documentary requirements. The most significant change resides in Article 81, which establishes the "requirement for an Importer of Record to provide documented support on the valuation of imported merchandise to the Mexican customs broker." Documents must be available at the time of importation to be provided to customs upon request. As written, the article makes importation cumbersome and sometimes impossible, as it asks for documents that are non-existent, confidential, or issued

after the import. Importers and customs expeditors continue to express concern with this requirement, not only because of the burden it imposes on companies, but also because of its potential to become a barrier to trade. ITI requests that USTR include this issue in the 2021 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.

In 2017, Mexico indicated that it was updating its product safety regulations for IT and electronic equipment under NOM 019 and NOM 001, respectively. At the same time, the Mexican Standards Agency (DGN) noted that it would no longer keep an equivalency arrangement under which it recognized testing to U.S. and Canadian standards for product safety. This indication has now become reality in late 2020, as Mexico seems to be unwilling to renew the unilateral equivalency arrangement that had been in place for years. As a result of equivalency becoming invalid, numerous products will require in-country testing and certification to Mexico's outdated product safety standards. To avoid expected bottlenecks and increased costs and delays at Mexico's local labs, ITI has proposed that Mexico leverage its existing membership in the IECEE CB Scheme. Under this arrangement, Mexico would need to update its standards and accept CB certifications and test reports in lieu of local testing and certification. These recommendations were rejected by Mexico. Although we understand that Mexico has its own sovereign right to establish guidelines on acceptance of foreign test reports for certification, we would ask that Mexico give a suitable transition time, at least one year, to address the challenges described above.

In February 2020, Mexico published a new conformity assessment procedure (PEC) on which ITI communicated a number of concerns regarding certain aspects of the procedure that are more trade restrictive than necessary to achieve the regulatory objective and could potentially pose technical barriers to trade. For example, the obligation to share with IFT test reports that may contain highly confidential product information (e.g., photographs, schematic diagrams) is of major concern as it jeopardizes confidential business information. The certification scheme consisting of models, families, and lots is likely to result in continuous and even parallel updates of the certificate of conformity, which would make import operations very complex and, in some cases, unfeasible. Also, in the newly published procedure, the number of samples is quadrupled for initial certification and doubled for surveillance. Taking into account that some of the samples would be high-cost equipment, this has the potential to increase industry costs considerably. Industry has conveyed to IFT a number of issues with the requirement for Importers of Record to have certificates of conformity in their own names. If conformity certificates become non-transferable, according to the published process, new conformity certificates would have to be issued to both manufacturers and distributors of products, thereby delaying the entry of products into the Mexican market. IFT has acknowledged in meetings with industry that the process is cumbersome, but claims that it is necessary for control in the import process.

In March, 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. 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 (6 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 2021 NTE will further emphasize the importance of these matters.

Mexican financial sector regulators - National Banking and Securities Commission (CNBV) and the Central Bank of Mexico (Banco de Mexico) - have issued Draft Provisions Applicable to Electronic Payment Fund Institutions (IFPEs). Article 50 of the Draft Provisions would impose data residency requirements on E-Payment Institutions (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 draft requirements to localize data run counter to the spirit, if not the letter, of USMCA's digital trade and financial services provisions. These draft 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, including, for the first time, foreign players. 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, known as the Conditions for the Interoperability of Clearinghouses (CICC), an industry agreement authorized by Banxico in Oct. 2014, relies 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 is still reflecting 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 to resolve this ambiguity, U.S. payment firms are 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. It is worth noting that this topic, among others, is part of a comprehensive investigation that Mexico's Competition Authority (COFECE) launched in 2018 on the potential existence of barriers to entry within the card payments system in Mexico, and on which COFECE is expected to issue a report in December 2020.

Since 2018, Banxico has played an important role in facilitating the dialogue among industry participants in search for a solution to enable existing and new payment networks to coexist in Mexico, which resulted in the industry agreement known as Iniciativa 28. The enforcement and implementation of this agreement is now crucial to provide certainty to all payment network participants, both current and new entrants. We urge USTR to ensure that Mexican authorities assist in the implementation of Iniciativa 28, eliminating current barriers to foster a competitive, level playing field for national and international participants, in compliance with Mexico´s commitments under USMCA.

Mexican financial sector regulators - National Banking and Securities Commission (CNBV) and the Central Bank of Mexico (Banco de Mexico) - have issued Draft Provisions Applicable to Electronic Payment Fund Institutions (IFPEs). Article 50 of the Draft Provisions would impose data residency requirements on E-Payment Institutions (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 draft requirements to localize data run counter to the spirit, if not the letter, of USMCA's digital trade and financial services provisions. These draft regulations create burdens for 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.

Nigeria

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.

On August 19, 2020, the Nigerian Identification Management Commission 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.

Key components of the draft Data Protection Bill:

- Scope of Bill 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 regualtory uncertainty regarding organisations' ability to transfer data across international borders
- Sensitive Personal Data currently includes any data relating to the behaviour of an individual, potentially creating restrictions on any data that may indicate a pattern of behaviour (such as online activity, browser usage, or payments history)
- Automated decisions currently require notification to the data subject whenever a "decision" is made about that individual; 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
- Data Protection Officer required (DPO)
- Fines of up to approx 15,000 $USD or imprisonment for up to one year for failing to comply

Pakistan

In February 2020, the Ministry of Information Technology and Telecommunication (MOITT) posted on its website the Citizens Protection (Against Online Harm) Rules.[10] 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 that a committee led by the Pakistan Telecommunication Authority would conduct an "extensive and broad-based consultation 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.

In May 2020, the Ministry of Information Technology and Telecommunication (MoITT) released a draft Data Protection Bill[11] which contains provisions on data localization (including an undefined "critical personal data" category), a powerful regulator in a newly established data protection authority, extraterritorial application, and criminal liability.

Data localization requirements:

- Data mirroring for all personal data
- On-soil processing for critical personal data (not yet defined) – no ability to transfer the data offshore

Key additional components:

- Financial data is classified as sensitive personal data and subject to additonal restrictions on processing
- Notice requirements – privacy notices must be in both English and local languages

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

- Penalties – financial penalty of up to 1% of annual turnover for non-compliance

Peru

In May 2020, the Digital Government Secretariat of Peru released for consultation a draft of Emergency Decree 007 - Digital Trust Framework regulations. The proposal appears to create unnecessary trade barriers for U.S. and other foreign service providers by giving preferential treatment to domestic data storage and domestic service providers. 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 digital service 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.

Philippines

The Philippines' national legislature is considering regulation of all internet transactions through the proposed Internet Transactions Bills (House Bill 6122 and Senate Bill 1591). The proposal 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 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.

Russia

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 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 Small and Medium Size Enterprises (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 labelled 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.

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 will require all technically complex, consumer facing products to have a select group of apps installed before being shipped for sale to consumers. The measure comes into effect January 1, 2021, and will discriminate against U.S. apps and impose discriminatory burdens on U.S. device manufacturers. ITI requests that this issue be raised in the 2021 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 on-line 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.

On November 1, 2019, the so-called Internet Sovereignty Bill took effect. The bill had been introduced in February 2019, and 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 will be incredibly 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.

South Africa

In order to mitigate against perceived sovereign risk, the South African Reserve Bank (SARB) has been reviewing the status of the processing of domestic transactions. A moratorium has been imposed by the Reserve Bank informally since 2013. Formally reinforced in July 2018, the moratorium prevents banks from migrating the switching of domestic transactions away from the local processing system operator to the international card networks. In August 2019, the SARB published its policy position which stated 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 remains in place until the SARB publishes the anticipated Directive on domestic processing.

The 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 (although the SARB is not opposed to cross-border data use, and supports cloud computing). 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. As a result of those conversations, SARB is now considering another one of the industry options for the Directive and has opened for industry consultation a hybrid model of allowing limited cross-border processing subject to certain volume thresholds. It aims to publish a Draft Directive for comments in Q4 2020. After comments are received and considered, the final Directive will go for approval by the Governors of the SARB, then final publication.

South Korea

In May 2020, the National Assembly adopted amendments to the *Telecommunications Business Act* and the *Network Act* to require value-added telecommunications services (VATS) providers operating in South Korea to appoint a local agent, take measures to ensure network quality, and potentially moderate content. In September 2020, MSIT and 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. VATS providers must also create a local presence with a hotline/call center operation for customers experiencing network issues,

which we believe runs the risk of conflicting with KORUS market access obligations. 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 KORUS obligations.

In October 2020, Korean legislators in the National Assembly proposed six bills that would amend the Telecommunications Business Act to ban app stores from requiring that app developers use a uniform billing system. While the proposals appear origin-neutral on the surface, Korean legislators have made clear through public statements that the legislative intent is to target U.S. firms, while favoring their Korean competitors. If enacted into law, the legislative proposals would restrict U.S. app stores' ability to charge a service fee through their own payment platforms, thereby limiting the ability to provide services in a safe, secure, and efficient way. Industry is concerned that the conditions imposed on U.S. companies by the proposed amendments would significantly impede affected companies' ability to supply global services on a cross-border basis to Korea, and would potentially run afoul of Korean market access and investment commitments under the Korea-United States Free Trade Agreement (KORUS). The conditions would also restrict U.S. app developers' ability to reach the Korean market via trusted U.S. ecosystems.

Though the Cloud Computing Promotion Act was passed in 2015, significant barriers still exist to the adoption of public cloud services, especially those that are provided from offshore locations. In 2016, the Korea Internet and Security Agency (KISA) created a cloud security certificate (KCSC) system governing public sector cloud service procurement. The KSCS is a key barrier for U.S. CSPs in the Korean public sector market as U.S. firms are unable to meet four components[12] of the certification. As a result, all central and local government ministries, affiliated public institutions, and educational institutions (from primary schools to universities) are prohibited from adopting cloud services offered by U.S. CSPs. The government has also begun requiring the certificate in other sectors, such as in healthcare, where the Ministry of Health and Welfare (MOHW) recently included new requirements for Electronic Medical Record (EMR) system providers who seek to use public cloud services. While MOHW claims that the certification is not mandatory, it plans to provide medical insurance reimbursement premiums only to medical institutions with certified EMR systems, thus creating an unlevel playing field for companies who are unable to obtain the certification. The KCSC system needs to be amended to allow Korean public sector institutions to adopt global CSPs' services.

In the shorter term, identifying public sector agencies and projects that can be exempted from the KCSC requirements will speed up the adoption of cloud services in the public sector. This can be achieved if the Ministry of Interior and Safety (MOIS) revises the *Guideline on the Use of Cloud Services in Public Sector Agencies* so as to minimize discriminatory KCSC requirements. Further,

[12] 1) Physical Separation (including physical resources; access control systems; supporting human resources);
2) Common Criteria (CC) certification of Hypervisor, Network Devices, VMs, and AWS Management Console;
3) Vulnerability Scanning (Vulscan) and Penetration Testing (Pentest) of AWS infrastructure; and
4) Use of Local Encryption Algorithm (i.e., ARIA, and SEED).

the Korean government limits the public sector agencies to only utilize specific encryption algorithms that are recognized by the government, excluding the widely used, internationally standardized algorithms.

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. multinationals. 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.

ITI appreciates the U.S. government's attention to the issue of spatial information and mapping data in South 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 South 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 2021 NTE.

While South Korea has been a member of the Common Criteria Recognition Agreement (CCRA) since 2011, since October 2014, the National Intelligence Service (NIS) has imposed additional domestic cybersecurity certification requirements through its Security Verification Scheme (SVS). The purpose of the CCRA is to ensure a uniform standard for product security assurance and remove the need for additional verification or certification between countries, save for applications which involve sensitive government systems. The South Korean government, however, has broadly imposed the SVS for internationally CC-certified information security products to be sold to the public sector. As purchasing Korean government and public sector agencies are required to conduct the verification process rather than the information security product vendor, this creates a significant disincentive for government procurement of foreign information security products.

Taiwan

Taiwan's National Communications Commission is consulting on a draft bill that would impose registration requirements on OTT service providers. The bill proposes broad requirements, including disclosure of subscriber numbers, appointment of a local representative, and

membership of a self-regulatory body, that would present barriers to foreign OTT service providers, including by requiring the disclosure of commercially sensitive data.

Thailand

Proposed OTT regulations would require online video services to register as broadcasters with the National Broadcasting and Telecommunications Commission (NBTC), even though online video services differ fundamentally from broadcasting services. For example, online video services do not use finite public spectrum and do not otherwise 'push' content into homes. These regulations would impose criminal penalties on businesses that continue to advertise on platforms that failed to register with the NBTC.

In July 2020, the Thai Industrial Standards Institute (TISI) officially announced that the current voluntary safety standard TIS 166-2549 (hereafter referred to as TIS 166), for plugs and socket-outlets for household and similar purposes, is now mandatory. ITI pointed out to TISI that this new announcement has an effective date of 120 days following the announcement date, to which TISI responded that the standard was notified in 2016. Although this is true, the 2016 notification did not include a date of adoption or entry into force as a mandatory standard. Even in normal operating times, 120 days is a very quick transition period for a mandatory standard that will require companies to undertake several significant steps, including re-design, development testing, qualification, in-country certification testing, phasing in of the certification mark, and final production. More specifically, because the standard has been voluntary for many years, most cordset suppliers do not yet have TISI approval to the standard and thus there is likely to be a disruption of business in Thailand. The speed at which cordsets are approved and shipped will be greatly dependent on lab capacity and supply chains, both of which are greatly complicated by COVID-19 impacts around the world. Furthermore, with factory inspections on hold due to COVID-19, we understand that TISI will issue temporary shipment-by-shipment approvals based on in-country test reports, which is a lengthy and cumbersome process.

In terms of product labelling TISI has plans to create a QR code for each license, and license holders must include QR codes on their products from the effective date in January 2021. We understand that this QR code requirement is retroactive to all TISI-approved products, including those that are certified by TISI prior to the QR code launch date. ITI conveyed to TISI that implementing new QR codes on product labels is a significant change and will require significant effort and time to incorporate into global supply chains. This is especially critical for products that are already TISI certified, as it will require delving into current products' designs and labelling to assert conformity, activities which will be nearly impossible to complete by January for already-certified products. ITI requested a minimum of six months to prepare for and implement any marking change, after the approved QR code format is provided by TISI (as of late October 2020, no format has been provided). High volume products would need an even longer transition time of around one year due to multiple manufacturing locations and distribution hubs that must be coordinated. We also requested that TISI apply good regulatory practices and perform full regulatory impact analyses, as well as consider the economic impact of any marking or QR code

requirement.

Turkey

The Presidential Circular on Information and Communication Security Measures No. 2019/12 published on 6 July 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.

Another sector-specific regulation imposing localization requirements for companies in the financial services industry is also expected to be enacted by the end of 2019. The draft regulation on the Information System of Banks and Electronic Banking Services prepared by the Banking Regulation and Supervision Agency is currently in the final review process. This regulation required banks and financial services to keep their primary information systems (production data) within the country.

Since March 1, Turkey has implemented a digital service 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) 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.

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) in July 2020. 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 Requests every 6 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 reduction to their platform. While these amendments aim to regulate social network providers and enhance the obligations of hosting and content providers in order to protect the individuals in the internet environment, the vague obligation of data 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.

In April and May, the government temporarily increased the customs duty for imported game consoles by 50% and introduced a 30% "additional customs duty" for a variety of intermediary and consumer goods imported through commercial channels until December 31. This applies to nearly 3,000 types of products, including technological devices, home appliances, industrial products, cosmetic and beauty products, musical instruments, building materials and textile products. These duties are imposed in the form of "additional customs duties" due to Turkey's obligations as a member of the Customs Union with the EU not to amend "customs duty" rates. Turkey has argued the duties are justified based on provisions of WTO Agreements allowing members to take measures to protect domestic industries.

United Arab Emirates (UAE)

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

Retroactive to April 1, 2020, the United Kingdom adopted in July a digital services tax (DST) 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.

On September 1, 2020, the UK Government published "Using the UKCA Mark from 1 January 2021" Guidance, which specifies that the UKCA mark will be required for all products currently having a CE mark starting January 1, 2021, with a grace period until January 1, 2022 that would allow import of products with a CE mark. Even though the UKCA mark requirements are the same as those for the EU CE mark, manufacturers must still utilize the UKCA mark as of the effective dates. This will require costly and time-consuming product redesigns throughout global supply

chains to add yet another compliance label to products. Meanwhile, this additional UKCA mark provides no additional information or assurance not already identified by the CE mark. ITI has requested that BEIS extend the existing stock exemption to goods "fully manufactured and ready to place on the market before" January 1, 2022 for system level products, extend the existing stock exemption to goods "fully manufactured and ready to place on the market before" January 1, 2023 for components, and eliminate the requirement to add the "BS" prefix to the EN standards to which the products have verified compliance.

Vietnam

Vietnam has increasingly considered or implemented 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. One recent study by the Brussels-based think-tank the European Centre for International Political Economy (ECIPE) stated that such a data localization requirement reduced GDP growth in Vietnam in 2014 by 1.8 percent. In May 2020, MIC proposed changes that would include a new set of regulations on cross-border transfer of public information, gives the government broad authority to force foreign compliance with take-down requests (with a window of 48 hours), and obliges domestic telecom firms to suspend service of foreign companies who fail to comply with take-down requests. Such requirements are overly stringent and difficult to comply with, along with specifically targeting foreign companies. ITI requests that the U.S. government again include this issue in the 2021 NTE.

On August 19, 2020, the Ministry of Information and Communications (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 February 2017, Vietnam's MIC introduced the Decree Amending Decree 72/2013-ND-CP (Circular No. 83) on the use of Internet Services and Online Information that includes an excessively short three-hour window for compliance with content takedown requests, as well as numerous other market access barriers highlighted below. The requirements in this decree deviate from international standards on intermediary liability frameworks, and present significant barriers to companies seeking to do business in Vietnam. Online services often require more than three hours to process, evaluate, and address takedown requests, particularly in situations where there are translation difficulties, different potential interpretations of content, or ambiguities in the governing legal framework. We encourage USTR to work with Vietnam and other countries to develop intermediary liability protections that are consistent with U.S. law and

relevant provisions in trade agreements, including Section 230 of the CDA, and Section 512 of the Digital Millennium Copyright Act (DMCA).

As with previous decrees, this draft decree also includes long and inflexible data retention requirements, a requirement for all companies to maintain local servers in Vietnam, local presence requirements for foreign game service providers, requirements to interconnect with local payment support service providers, and other market access barriers that will harm both U.S. and Vietnamese firms. We urge USTR to press Vietnam for changes to this decree and for greater transparency and public input into the development of Internet-related proposals.

In June 2018, the Ministry of Public Security finalized its Law on Cybersecurity (LOCS), which 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 July 2019, Vietnam also released the second version of a draft Implementing Decree outlining further measures as a result of the LOCS that creates an even more expansive and problematic approach to data localization. The latest draft implementing decree was reportedly discussed by the Cabinet in August 2020 and has been privately shared with select foreign governments. Within this draft, there is a provision that would require all domestic companies to keep their data in-country, while foreign companies would only have to onshore their data if they do not adequately cooperate with law enforcement. Technically, this Law applies equally to local and foreign companies. However, if all domestic entities are required to localize data under this implementing decree, hyper-scale CSPs, which generally lack a necessary local presence, will not be able to sell to Vietnamese customers. On the other hand, if localization mandates are issued to foreign entities with no local presence, these foreign entities will incur significant additional overhead costs vis-à-vis their local competitors.

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 cyber security 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.

As a general matter, new MIC requirements provide unreasonably short transition times and some important measures are not notified through the TBT Inquiry Point (such as the publication of Circular 10/2020/TT-BTTTT, which became effective on 1 July and includes some major changes in certification method for products and goods). However, we have seen improvement from MIC in terms of responses to some of our queries, though the Ministry of Science and Technology (MOST) continues to ignore our requests. ITI continues to engage with MIC and MOST, through the TBT Inquiry Point when measures are notified. Further U.S. assistance in persuading agencies to respond to requests for clarification and to implement reasonable timeframes would be beneficial.

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 control cross-border digital platforms. The Ministry of Information and Communications (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 […]"(1). While these standards are technically "voluntary," in practice, this will be adopted by the Vietnamese public sector as if it is mandatory.

The Tax Administration Law, effective July 1, 2020, taxes cross-border e-commerce and other digital services. The Ministry of Finance is drafting the implementation circular, which will mandate that cross-border digital service providers register, declare and pay taxes (VAT and corporate income tax) from January 2021 (the official release of a draft circular is forthcoming). Pending outcomes in the OECD project, unilateral taxes applied by Vietnam will put U.S. companies at risk of double taxation and create tax compliance burdens.

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. In July 2020, Vietnam issued a draft amendment to the Non-Cash Payment decree, which includes the following changes: removes regulations on mobile money, removes the 49 percent cap of 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 State Bank of Vietnam. These measures would appear to require NAPAS to obtain written approval from the SBV to connect to U.S. electronic payments companies. 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).