ITI Promoting Innovation Worldwide

October 31, 2019

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.

2019 was a landmark year in U.S. digital trade policy. In USMCA's digital trade chapter, USTR has established a model for ambitious commitments to counter barriers to digital trade. Similarly, the conclusion of a bilateral Agreement on Digital Trade with Japan enshrines strong commitments to maintaining open digital trade among two leading innovation economies, and provides an example to which third countries should aspire. Finally, active U.S. engagement in the WTO Digital Trade Initiative has helped advance 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, impeding U.S. exports of goods and services across a wide range of sectors. 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 2019 NTE made significant improvements on previous iterations in addressing many policy priorities for the tech sector, particularly forced localization policies and 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 improve the trading relationships with our partners. We are confident that the 2020 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:

1. **Take action against digital trade restrictions that inhibit greater trade in technology products and services**. U.S. trade officials must both combat foreign trade restrictions that impact the technology sector and other sectors that use technology, and fight 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, or infrastructure; (d) countering discriminatory, unilateral digital taxation measures; (e) ensuring that governments

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

implement safe harbors to protect Internet services from liability for activity by third parties; (f) 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; (g) prohibiting the extension of domestic telecommunications and broadcasting regulatory and licensing requirements to online services and applications; and (h) prohibiting forced transfers and disclosure of technology, source code, algorithms, or encryption keys. Addressing these items would have a large impact on the tech sector's ability to export both goods and services to foreign markets, maintain the United States' status as the leading market for innovation, and increase the number of jobs created domestically.

2. **Enforce U.S. trade agreements to ensure our companies and workers can compete fairly.** The rules in our 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 therefore encourage an active and aggressive approach to enforcement of U.S. trade agreements, targeted at problems of significant concern. Similarly, we support USTR's engagement to counter discriminatory, unilateral digital taxation measures. We appreciate opportunities to engage with USTR to discuss our 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. 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 we feel 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 and 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. USTR took a complementary and important step of creating an internal working group on digital issues which we believe merits continued support and resources. We remain committed to working with USTR and other agencies as a whole-of-government approach is adopted 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 VAT on information technology and electronic products, including mobile phones, cameras, and tablets produced outside the Special Customs Area within Tierra del Fuego province. 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.

Electronics and Electronic Waste (WEEE) is an area in which a patchwork of laws, regulations, and other requirements are increasingly common. Such requirements—which confuse consumers, who are key stakeholders in recovering WEEE—unnecessarily impact the manufacturing, marketing and business models of the electronics industry without affording greater environmental protection. Consistent national, rather than regional or local, requirements facilitate consumer participation and industry compliance, establish a level playing field among producers, and avoid unnecessary costs that could be better invested in enhancing industry take-back programs. The City of Buenos Aires requires a specific symbol for environmental purposes. Buenos Aires Provisional Law No. 14321*, Sustainable Management of Electrical and Electronic Waste* (*Ley Provincia de Buenos Aires Nº 14321, Gestión Sustentable de Residuos de Aparatos Eléctricos y Electrónicos*) requires an environmental crossed bin symbol the product and packaging. That label is only required in the City of Buenos Aires. Though this law has been passed, no implementing regulations have been drafted. As such, ITI requests that USTR watch this issue closely and encourage Argentina to create national WEEE standards instead of allowing city-specific standards.

ITI appreciates the United States government's efforts to ensure Argentina's compliance with the WTO case regarding its use of import licenses to restrict imports. We encourage the U.S. government to pay close attention to Argentina's actions and to continue to ensure that the Comprehensive Import Monitoring System (SIMI), which has replaced the DJAI system, does not serve as a barrier to trade.

An additional challenge with the SIMI that e-commerce companies already observe is related to the low-value import regimes (Postal, Express, and General). Currently, only the Express regime serves as an option for e-commerce transactions, but the limits within the Express regime create serious roadblocks for U.S. companies seeking to export to Argentina. The Express regime limits shipments to packages under 50 kilograms and under $1000, with a limit of three of the same items per shipment, with duties and taxes assessed. While import certificates/licenses for products are not required, the government limits the number of shipments per year per person to five, which is strictly enforced. This creates burdensome compliance obligations for companies that have large e-commerce businesses in the country.

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 is currently reviewing issues and concerns observed during the first year of the law's implementation (concluding in December 2019). This will be an important juncture at which industry and the Australian government can assess the impact of the law and correct any issues.

The Criminal Code Amendment (Sharing of Abhorrent Material) Act was rushed 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.

Brazil

ITI remains extremely 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'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.

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 information and communication technology (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 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 both Business to Consumer (B2C) and Business to Business (B2B) transactions. There is some legal disagreement in the way that the rule is being interpreted; there exists some case law stating that the exemption should apply for both B2C and C2C transactions and that the *de minimis* threshold should be raised to USD $100. This varied treatment of the threshold between transactions and the low *de minimis* threshold for imported items creates unnecessary barriers to trade through increased transaction costs for Brazilian businesses, and acts to restrict consumer choice and competition in the Brazilian market. ITI requests that the U.S. Government address this barrier to trade in the 2020 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.

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.

Finally, 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.

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." 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 the United States-Mexico-Canada Agreement ("USMCA"), which generally prohibits the parties from restricting the flow of personal information between one another (Art. 19.11).

Canadian Prime Minister Justin Trudeau has 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. ITI urges USTR to seek to prevent Canada from formally proposing this unilateral DST measure, which would run counter to commitments in both NAFTA and USMCA.

Chile

Chile is regulating the testing and certification for safety for an increasing number of electronics and ICT products. There are also requirements for Chile-specific labeling of electronics and for certain safety or alert systems that differ from industry standards. One key example of this is Resolution 1179, which changes processes for labeling, testing, and registering cell phones in the country. Many of these new requirements have been imposed without a regulatory impact assessment or sufficient stakeholder consultation.

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 2019, Chile issued Public Consultation PE Nº 8/9:2019, regarding the extension of the rule for many other power adaptors that include 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 IECEE CB scheme.

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 2020 NTE and urge China to uphold the international commitments that it agreed to when joining the WTO.

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 may compel companies to disclose sensitive information and create an environment conducive to uneven enforcement. The Law also still contains "secure and controllable" requirements, which were raised in the 2016-2019 NTEs as a known issue with serious implications for domestic preferences.

Data localization measures remain problematic in China, jeopardizing not only the technology industry, but all other industries that depend on ICT platforms for global operations. 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.[1] For instance, even though U.S. cloud service providers (CSPs) have stimulated innovation and application of cloud services around the world, China has imposed several onerous regulations on U.S. CSPs - effectively barring them from operating or competing fairly in China. Enforcement of Chinese laws and regulations on non-Chinese CSPs can force U.S. CSPs to unwittingly expose valuable intellectual property, surrender use of their brand names, and hand over operation and control of their businesses to Chinese companies to operate in China.

Embedded within the Cybersecurity Law and among numerous regulations and standards are requirements to store, process, or manage data locally within China and restrictions on the flow of data out of China. The most tangible restrictions are found in the *Measures on Cross-Border Data Transfer*. The CSL creates additional barriers by mandating data localization for critical information infrastructure (CII) network owners and operators in China and restricting flows of data out of China. The *Critical Information Infrastructure Protection Regulation* – which should define CII and what type of data shall be localized – has been in draft for over a year.

These measures directly affect the ability of many industries beyond the tech sector to conduct normal business operations. This trend toward increased control over where and how data is transferred represents a misguided attempt to protect Chinese tech companies from foreign competition. What's more, other nations have begun to mirror these flawed policies, following China's lead. Implementation and enforcement of such policies is not realistic, especially in smaller markets – leaving the door open for uneven enforcement targeting foreign companies.

China also continues to flout international standards and norms, as demonstrated by an increase in laws and standards that include China-specific requirements. In 2018, China finalized its

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

Encryption Law, which currently requires unique encryption of products and services within China that does not align with the Common Criteria.[2] 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.

China also finalized its Standardization Law in late 2017, which the government has used to create an increasingly burdensome standards regime. 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. Modification of products and services for individual markets is not only costly, but it also creates interoperability issues that may not allow consumers to use a specific product or service across markets with different standards. In coordination with industry, the U.S. government should continue to encourage China to participate in rules-based international standards development bodies, where they can work with other companies to develop standards that are most appropriate for the current technology and consumers. Further, we encourage the U.S. government to work with other nations to discourage China from creating unique standards and instead rely on *voluntary* international standards.

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.

In recent years, the Colombian Regulatory Commission (CRC) has produced more than 20 resolutions to create a complicated system of black (mobile phones reported as lost or stolen) and white (mobile phones with homologation, valid International Mobile Equipment Identity - IMEI) lists. ITI urges the U.S. Government to encourage the CRC to explore other less intrusive approaches, like educational campaigns about technology-based solutions (such as those that allow the user to block the phone, remotely erase the content, and make the devices unable to connect to the network), enforcement, and cooperation beyond national borders.

Recent efforts have been made by the Superintendency of Industry and Commerce, the consumer protection authority in Colombia, to amend its "Circular Única" requiring all mobile

[2] 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.

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.

Ecuador

Tariffs on several technology products, including computers, tablets and smartphones in Ecuador were high in the regional context, and were recently eliminated by a decision of the Trade Committee (COMEX). In its decision, COMEX instructed the Ministry of Telecommunication to present a report every semester and verify that the benefits of this reduction were passed onto consumers. ITI urges USTR to encourage Ecuador to promptly implement this decision.

European Union

The European Commission's Digital Single Market (DSM) Strategy includes numerous elements that could help build consumers' and businesses' trust in technology and create a more integrated market in Europe for innovative technologies. As the Commission and Member States move forward with DSM implementation, they should take care to advance these laudable goals while maintaining an inclusive environment for ICT products and services from both within and outside Europe.

The U.S.-EU Privacy Shield arrangement, which took effect on August 1, 2016, was recently reaffirmed by the European Commission and the Commerce Department following the third joint annual review. This arrangement represents a strong commitment by both the U.S. and EU to enable transfers of data across the Atlantic and safeguard consumer privacy. However, threats to transatlantic data flows remain primarily due to: 1) the pending judicial review at the European Court of Justice of standard contractual clauses, which give U.S. companies an alternative option to ensure that they can transfer data from the EU to the U.S., and; 2) challenges in other EU courts to the Privacy Shield itself.

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. 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 is in 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.

ITI is closely monitoring several legislative initiatives in the EU which seek to regulate various aspects of emerging technology. In spring of 2019, the EU finalized the Cybersecurity Act, which establishes a framework for the creation of cybersecurity certification schemes for different products, services and processes with cybersecurity risk profiles. These schemes are to be initiated by the European Commission and developed sequentially by the European Union Agency for Cybersecurity (ENISA). ITI will remain engaged in monitoring and providing input regarding the implementation of the Cybersecurity Act and the development of certification schemes. We urge the Commission to avoid developing any mandatory or overly prescriptive requirements, and to base schemes on global, industry-driven, voluntary-consensus standards to avoid harmful market fragmentation.

In addition to such horizontal regulatory approaches to emerging technology, the European Commission has also proposed regulating aspects of emerging technology through revisions to existing vertical legislation. The Commission is currently developing an impact assessment to determine whether and how to revise the Machinery Directive. The assessment contemplates changes to the Directive's essential health and safety requirements to "explicitly address aspects relating to emerging digital technologies, e.g. AI, cybersecurity, IoT." ITI believes that any such new requirements would be redundant, as the Machinery Directive's existing essential requirements already require that manufacturers account for all potential risks, including those associated with the use of more modern technology. Moreover, given that product legislation aligned with the New Legislative Framework (NLF) is intertwined, the vertical regulation of emerging technology risks creating legislative inconsistencies and unnecessarily restrictive requirements. A revision to the Machinery Directive could take the form of an updated Directive or could entail conversion of the existing Directive into a Regulation, thereby rendering it directly applicable at the Member State level.

The Commission is also assessing several 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. It is unclear how such requirements, if incorporated into a vertical directive, would interact with existing, broad-based requirements for privacy, as well as forthcoming cybersecurity requirements developed under the Cybersecurity Act. 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 has developed an impact assessment regarding a common charger for mobile devices. 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. The Commission could issue a proposed delegated act as soon as late 2019 or early 2020.

Lastly, we remain deeply concerned with the enactment of a unilateral, digital services tax (DST) by France, as well as the introduction of DST measures by six other individual EU Member States and the Commission's indication of the potential for renewed DST efforts at the EU level in the absence satisfactory political agreement is not reached as part of ongoing deliberations at the Organization for Economic Co-operation and Development (OECD). As outlined in detail in ITI's submission in response to USTR's Initiation of a Section 301 Investigation of France's Digital Services Tax, the design of the French DST and comments by French senior officials prior to and following its enactment strongly suggest that the measure is discriminatory in nature. We encourage USTR to continue to use the NTE to raise the significant trade-related concerns posed by all unilateral digital services taxation measures, including those put forward to date in France, Austria, Spain, Italy, the United Kingdom, Czechia, and Poland.

In December 2017, the 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. 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. Further guidance is needed to provide clear advice and mechanisms to businesses who want to comply and to ensure that implementation of the Regulation is consistent with the EU's obligations under the WTO TBT Agreement.

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 cross border 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 relevant EU legislation takes the form of directives, country implementation is not harmonized. As an example of the resulting complexity, 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 28 jurisdictions, under 28 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, which tend to be minimal). 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 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.

Hong Kong

The Hong Kong Department of Environmental Protection has mandated the use of a unique electronics recycling label. Companies must file with the government an issuance application for all electrical and electronic equipment. There are alternative and more effective methods for communicating recycling information, such as electronic labeling or real-time information on websites. Hong Kong's unique recycling label adds cost and logistical transport complexity without furthering environmental policy goals.

India

India's digital ecosystem is rapidly degrading for American companies. ITI is concerned about India's increasingly restrictive data policies policy which 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 2020 NTE as well as through direct bilateral discussion.

In April 2018, the Reserve Bank of India (RBI) released a one-page directive on the Storage of Payment System Data that required all payment data to be stored only in India within six months without any prior stakeholder consultation or notice. Despite extensive efforts from industry to engage RBI and seek technical clarifications, the RBI was unwilling to address industry concerns. U.S. payment companies ultimately made significant investments to adhere to the regulator's demands. Meanwhile there is growing evidence that the Government of India is creating an un-level playing field for U.S. firms operating in the market both through overt political statements of support for "homegrown" providers, and policies and projects designed to promote the use of domestic payment solutions in lieu of U.S. branded solutions. One such example is the National Common Mobility Card (NCMC), where the Ministry of Housing and Urban Affairs (MoHUA) has issued directives limiting participation to card networks that use RuPay's proprietary specifications, effectively shutting out global payment networks. As India continues to develop policies and projects intended to spur the use of digital payments, it is imperative that U.S. firms

remain eligible to compete for these opportunities on a level-playing field with their domestic counterparts.

In August 2018, the Government of India released a draft Data Protection Bill that would prohibit cross-border transfers of personal information except when certain criteria are met. Even when those criteria are met, a copy of all personal data would still have to be stored in India. In addition, the bill would establish a committee that would designate certain data as "critical" which would prohibit cross-border transfers of that data in any circumstance. Though this bill appears to have been updated, the new draft has not been made public.

In February 2019, the Department for Promotion of Industry and Internal Trade (DPIIT) released the draft National E-Commerce Policy which, among other 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. Though the future of this policy is unclear, the Government of India continues to look into data-related regulatory frameworks as evidenced by the creation of a new Expert Committee that will explore regulating non-personal data.

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 2017, the Ministry of Electronics and Information Technology (MEITY) expanded the CRO to cover additional products; however, it failed to perform any risk or regulatory impact assessment to justify these additions. Market surveillance continues to be a challenge as companies struggle to deal with unworkable compliance requirements. Though industry stakeholders have provided MEITY with detailed recommendations to align the surveillance program with global norms, no significant changes have been made. We recommend that USTR continue to highlight these issues in the 2020 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. In September of 2018, India started seeking to change its tariff schedule through a schedule rectification in order to remove bindings on products for which it wishes to raise tariffs. 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 2020 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. The government recently filed an affidavit in the Supreme Court stating that it is likely to complete the process of notifying the revised intermediary rules by Jan 15, 2020. These amendments 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. We recommend that USTR engage directly with the Government of India on this issue and monitor closely, as new requirements could significantly impact the ability of American online services to do business in India.

Another pressing concern for the tech sector is India's restriction on the importation of refurbished and used goods ICT equipment. Since 2013, the Ministry of Environment, Forests, and Climate Change (MOEFCC) had been applying importation procedures for e-waste and hazardous waste to imports of used spare parts and whole equipment. In July 2015, MOEFCC went further and issued a Ministerial Decision, rejecting a significant range of used equipment and parts. On July 16, 2015, the MOEFCC published an Official Memorandum regarding imports under the India Hazardous Waste (Management, Handling and Transboundary Movement) Law 2008, which effectively banned importation of used, secondhand and refurbished computer parts and components. MOEFCC subsequently rescinded this Official Memorandum in August. Despite this reversal, ITI member companies' used equipment shipments are not approved for importation by the Government of India and they must go through a burdensome exemption process to be imported. 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 2020 NTE to push the government of India to clarify if and how it will enforce this regulation.

Lastly, cloud service providers 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. cloud service providers 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.

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 recently passed 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, we continue to have concerns around discriminatory treatment of U.S. firms as Indonesia seeks to develop cybersecurity policies. Indonesia's government is drafting of a Cybersecurity Law which provides for the possibility of certification schemes that may discriminate against foreign firms operating in Indonesia. 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 information flows into Indonesia. The inclusion of "software and other digital products transmitted electronically" in Indonesia's HTS skirts Indonesia's commitment under the World Trade Organization (WTO) Moratorium on Customs Duties on Electronic Transmissions, a commitment that Indonesia reaffirmed as recently December 2017. 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 would encourage continued engagement with the Indonesian government to resolve it.

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 based on the limited number of local labs that can conduct the tests. Currently, the regulation specifies that SDPPI will only accept foreign test reports until January 2020, a deadline that has been extended several times before. Industry has encouraged SDPPI to continue to accept international test reports indefinitely. Absent that change, we have encouraged the Agency to provide necessary certainty by extending the period during which it will accept international test reports by another 1-2 years.

Similarly problematic are two regulations recently released by KOMINFO, No. 9 of 2019 (Wavelength Division Multiplexing) and No. 10 of 2019 (Internet Protocol Networks), both of which include a requirement to "meet the Domestic Component Level in accordance with statutory provisions." No previous notice was given for this local content requirement, and no specifics are provided on the levels that must be met. In order for manufacturers to meet any sort of local content requirements, notice must be given very early in the process so that manufacturing processes, supply chains, and other necessary accommodations can be established. We continue to seek additional information on the compliance requirements of both measures, and anticipate that U.S. companies will face significant additional compliance costs.

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. We have requested from SDPPI, via letter to the Agency, at least a one-year transition time for any new regulation, a time period that is practical and achievable with reasonable assurance of uninterrupted market access of products. Finally, industry has encountered regulations or standards where the requirements are vague or unclear. Establishment of an inquiry point in SDPPI to field such questions would greatly facilitate industry compliance. Several of these issues have been communicated to the SDPPI via a letter from ITI, but inclusion of the issues in the 2020 NTE will further emphasize their importance.

ITI was pleased to see USTR address Regulation 27/2015, *Technical Requirements of Equipment and Telecommunication Devices Standards-based of Long-Term Evolution (LTE) Technology* in previous reports. We hope that USTR will continue to press Indonesia on this and related

regulations described below. In addition to a more recent regulation – Regulation 65/2016—Regulation 27/2015 imposes strict local content rules on 4G LTE smartphones, laptops, tablet computers, and all related equipment. These requirements are being phased in over the next few years, progressively raising costs and pushing out U.S. industry. In February of 2016, the Ministry of Trade (MoT) held a public hearing to socialize a new draft amendment for MoT Regulation 82/2012. This amendment rolls back many restrictions on investing and importing mobile phones into Indonesia, but it would still bar importers from selling directly to the consumer and would require some importers to obtain a "recommendation" from MoT in order to import. These types of measures will not help Indonesia meet any of its broadband or mobile connectivity objectives and will make it harder for local companies in Indonesia to operate and innovate.

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.

Finally, 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.

Kenya

The Kenyan Ministry of ICT has started drafting a new national ICT policy in response to, among other things, the need to provide clarity on how to treat OTT services. ITI was pleased to see that the draft of this policy acknowledged the importance of global OTT service providers' contribution to the local economy and recognized that OTT services "are one of the main drivers of internet adoption by consumers." We encourage the U.S. government to monitor the development of this policy and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach.

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. 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.

Mexico

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), mandate 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. SAT has delayed the enforcement of this requirement several times, most recently to January 15, 2020. 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 2020 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. As a result of these changes, ITI expects that 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.

Furthermore, the Government changed the Standard Annex (*anexo de normas*) of the general rules for trade, altering requirements for self-use, prototypes and samples, making it necessary to provide documentation of certification for all products in scope of NOM 019 and NOM 001. This has caused a significant adverse impact on trade of the affected products, causing delays and even preventing import in some cases. Though an existing equivalency arrangement should provide some relief, there have recently been instances where Mexico Customs officials have rejected shipments at the border, due to a misunderstanding of the provisions of the arrangement. ITI has reached out to the U.S. Government for assistance in addressing these instances.

Mexico is grappling with issues involving digital services and content, and several bills pending in the Congress would impose local content requirements and/or taxes on digital services and products. As part of 2020 budget legislation, one bill would require services that facilitate intermediate business transactions between users withhold VAT and income tax, and would disproportionally affect U.S. industry. Among these provisions are:

- Requirements for non-resident companies that provide digital services to customers in Mexico to keep a record of, and share, potentially sensitive information. Simple and clear documentation can provide a summary of the sales and tax collected, without revealing confidential customer information.

- The Collection of a Value Added Tax (VAT) when a customer is deemed to be in Mexico when one of three considerations is met. Requirements to determine a customers' location should not be overly onerous and should take into account typical customer information already collected by businesses and avoid double taxation.

- Obligations for marketplaces in which intermediate businesses between users to withhold VAT and income tax. This process is likely to be complex and difficult to administer and comply with.

- A “kill switch” provision to suspend the internet connection of non-resident entities to Mexico for noncompliance, which disproportionately affects U.S.-based companies.

Nigeria

The Guidelines for Nigerian Content Development in ICT (“Guidelines”), issued in draft form in 2014, require both foreign and local businesses to store all their data concerning Nigerian citizens in Nigeria. They also establish local content requirements for hardware, software, and services. In October 2015, the Nigerian Government issued a notice mandating compliance with the Guidelines by December 3, 2015. These rules damage U.S. business interests by greatly increasing the cost of entry to the Nigerian market, imposing discriminatory rules on hardware sourcing, and incurring unanticipated costs on already established business operations. We request that the U.S. government continue to address the gravity of the costs of the Guidelines in the 2020 NTE and continue to monitor the development of this policy closely.

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 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 (SME), 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.

In January 2016, the Kremlin issued a 16-point plan for improving the competitiveness and security of the Russian ICT sector through import-substitution, increased surveillance capabilities, and increased education on issues related to cyber. The plan is focused on import substitution and has generally been talked about in the context of “internet sovereignty.” Two new executive decrees associated with this plan call for ministries to create plans that: prioritize Russian-produced software and equipment for government purchases, create additional obligations for how the personal information of Russian citizens is processed, regulate the encryption of data, reorganize federal cyber-threat monitoring, and establish a Center of Import Substitution for

Information and Communication Technologies. In October 2016, a bill was introduced in the Duma that would further require government entities to provide preferences even to Russian developed software that is based on foreign-developed middleware. Further implementation and follow-up decrees have been opaque and seemingly poorly coordinated, so there is little information on how the plan has progressed. ITI requests that the U.S. Government continue to closely monitor the development of this plan and highlight its potentially discriminatory elements in the 2020 NTE and its annual assessment of Russian compliance with its WTO commitments.

Federal Law No. 149-FZ "*On Information, Information Technologies and the Protection of Information*," as amended in 2014, has two particularly troubling elements. First, Article 10.1 "*The Duties of an Organizer of Dissemination of Information on the Internet*," requires "organizers of the distribution of information on the internet" to retain all metadata within Russia for six months and provide access to that data to security agencies. This applies to an incredibly wide range of companies that facilitate the receiving, transmitting, delivery, and or processing of electronic messages—including any email and internet-based messaging services. Second, Article 10.2, the "Blogger's Law," requires bloggers with more than 3,000 daily users to register with Roskomnadzor and places restrictions on what they can and cannot post to their website. This law not only has significant free speech and human right implications, but it also creates costly barriers for U.S. companies who wish to do business in Russia.

These concerns were further exacerbated when, on July 7th, 2016 President Putin signed a package of laws (374-FZ and 375-FZ) that amended Russian Federal Laws 126-FZ and 149-FZ—known as the "*Yarovaya Amendments."* These amendments require "organizers of information distribution on the internet" to store the content of communications that they enable within Russia for 6 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 in 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 domestic telecommunications companies have been in vocal opposition to the law, a rare event in the country.

Finally, Russia applied new restrictions on foreign providers of audiovisual or online video on demand services in its so-called "VOD Law," which entered into force on July 1, 2017. The VOD Law applies to video on demand services that: (1) distribute audiovisual works via the Internet; (2) require customers to pay a fee or view ads in order to access audiovisual content targeted to Russian end-users; and (3) are accessed by more than 100,000 users located in Russia within a 24-hour period. The VOD Law also introduces foreign ownership restrictions on VOD services in Russia. Under the law, non-Russian entities are not allowed to own, manage or control more than 20% of the equity share in a regulated VOD service, unless (i) fewer than 50% of the end users of the service globally are Russian, and (ii) the service obtains a discretionary exemption from a Russian government commission established under the law. The VOD Law states that such exemptions would be granted based on the commission's determination as to whether the given VOD service "will facilitate the development of the audiovisual services market in [Russia]." This

discriminatory measure significantly restricts the ability of U.S. companies providing VOD services to do business in Russia and should be included in the 2020 NTE.

South Korea

Recent draft amendments from early 2019 on the *Act on Promotion of Information and Communications Network Utilization and Information Protection* from MSIT would require all online service providers to establish servers and data centers in country. These measures remain pending in the National Assembly. We urge USTR to press the Korean government on these and other policies that encourage data localization.

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[3] 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 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.

Under the *Credit Supervision Regulation*, e-commerce firms selling goods in Korean *won* are prohibited from storing Korean customers' credit card numbers in company information systems. As a result, U.S. electronic commerce firms unwilling to develop Korea-specific payment systems have been prevented from entering the Korean market. In November 2013, the Korean Financial Services Commission amended regulations to partially address this issue, a positive step that gradually moves Korean regulation in this area in line with global norms. Restrictions remain, however, and the latest innovations in financial services cannot be offered cross-border, which harms both U.S. companies and Korean consumers.

In the payments services sector, the Korea Credit Finance Association announced support for developing a local technology standard for Contactless Payment and Near Field Communication (NFC). This proposal raises concerns as it would conflict with international standards for global interoperability of payments technology. Using local instead of international standards disintermediates U.S. firms, which reduces investments in payment security and innovation, and

[3] 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;
4) Use of Local Encryption Algorithm (i.e., ARIA, and SEED)

depresses international consumer spending in cross-border travel and tourism.

Furthermore, 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 $220,000, while most local companies can bid on the majority of projects available. This is particularly problematic for foreign-invested 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 the 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.

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 2020 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.

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 business that continue to advertise on platforms that failed to register with the NBTC.

Turkey

In 2014 Turkey passed the E-Payment Law, requiring companies to process all digital payment transactions initiated in Turkey in data centers within Turkey's borders. This data localization requirement acts as a high barrier for entry into the Turkish market for SMEs and impedes the ability of U.S. firms to bring global innovation and security, impacting the operations of all companies in Turkey whether foreign or domestic. This law has been enforced strictly: the implementing agency is the Banking Regulation and Supervision Agency (BDDK), which has been canceling licenses to operate in Turkey when foreign companies have not complied. ITI requests that the U.S. government continue to include this law in the 2020 NTE, appropriately reflecting the economic impact it has on companies operating in Turkey.

Since there is no specific regulation dealing with the provision of cloud services, the Law on the Protection of Personal Data No. 6698 is considered to serve as the main regulatory framework in this respect. In addition to the data protection regulations, there are certain sector specific regulations scattered among diverse regulations which, in general, require entities operating in such sectors to use localized information systems.

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.

The Turkish Parliament may soon vote on a digital service tax of 7.5% 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 and threshold of the tax. It appears that the Ministry of Finance and Treasury is not waiting for OECD negotiations before passing this bill.

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.

UAE implemented a RoHS-type directive in 2018 requiring in-country certification. This was partially pre-empted by the Gulf Cooperation Council (GCC), and at this time it is unclear if the scope of the GCC requirements are the same as UAE. ITI would welcome further U.S. engagement on this issue to clarify the UAE requirements.

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. ITI requests that the U.S. government again include this issue in the 2020 NTE.

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.

Decree 6 from MIC on the management, provision, and use of radio and television services is currently up for revision. Following several drafts between 2017-2018, MIC released a fifth draft of the revision that contained significant restrictions on over-the-top (OTT) services. While the latest revision appears to have taken out explicit references to OTTs, the vague scope and mandate of the revision is still likely to capture many OTT services and has the potential to create restrictions on foreign company participation in the market. The U.S. Government should continue to resist any efforts that would prevent foreign competitors (including OTT services) from providing or supplying Internet services in Vietnam without a commercial agreement with local telecommunications companies.

In June 2018, MIC also 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.

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 letters and requests for clarification to MIC have gone unanswered. As an example, MIC released Circular 05/2019/TT-BTTTT dated July 9, 2019 to replace Circular 04/2018/TT-BTTTT. Effectively,

the new circular meant that companies would have to renew test reports according to new standards within 54 days. The short timeframe is partly due to the fact that MIC failed to provide notification of the circular to the WTO TBT Committee. A letter to MIC explaining the impacts of these actions and proposing an alternative path was never answered. ITI requests the U.S. Government's assistance in holding Vietnam to its WTO notification requirements.

MIC also plans to overhaul its conformity certification scheme, raising many questions around the scope and timeframe for the changes. Additionally, the Ministry of Science and Technology (MOST) has issued a draft regulation that would incorporate secondary battery and power banks into its existing, mandatory safety testing program. Inquiries to MOST have resulted in conflicting interpretations about the scope of the program. ITI continues to engage directly with MIC and MOST, and further U.S. assistance in persuading agencies to respond to requests for clarification and to implement reasonable timeframes would be beneficial.