# Table of Contents

October 27, 2016

## 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 that interested persons submit comments to assist in identifying significant barriers to U.S. exports of goods, services, and U.S. foreign direct investment for inclusion in the NTE.

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. We hope the new Digital Trade Working Group within USTR will act as a focal point for the US government in pushing back against digital protectionism. This broad term encompasses the wide range of government measures that in practice degrade the revolutionary benefits of the internet to all economic sectors across the globe. The NTE serves a powerful tool for highlighting how these measures impact the ability of U.S. companies to trade products and services and invest in overseas markets. In this light, we also hope that our NTE submission gives the Digital Trade Working Group an initial set of priorities as it pursues its work, particularly during the Administration transition in 2017.

*Localization Barriers to Trade*

ITI appreciates that this year's NTE Request for Comments has emphasized localization barriers to trade. ITI's member companies are contending with a proliferation of such barriers as many foreign governments attempt to foster their own domestic tech industries. While these measures are wide-ranging, we are alarmed at the sharp increase in number and forms of data localization requirements and other measures that attempt to control the free flow of data across borders. These measures not only have a dramatic impact on how and where tech companies can do business, but also negatively impact the operations and competitiveness of all sectors locally and globally. Pursuant to the Request for Comments, ITI's comments highlight localization barriers to trade in each foreign market below.

*Data Protection as a Barrier to Trade*

ITI has consistently been a defender of citizens' privacy, and of governments' right to regulate for the protection of that privacy. However, companies have increasingly encountered data protection regulations that include restrictions on data transfers. In our view these regulations are either poorly crafted or are based on the assumption that the transfer of data outside national jurisdictions compromises privacy. ITI recognizes that protecting privacy is in the global public interest and privacy breaches have a negative impact globally. Data protection mechanisms, therefore, while aiming to offer a high level of privacy protection should also aim to be easily implementable, and have potential for widespread adoption.

ITI has been deeply involved in the U.S.-EU Privacy Shield process, and, though the Privacy Shield is a good solution for the transatlantic relationship, it is not scalable to a global, multilateral level. The Asia-Pacific Economic Cooperation (APEC) forum's Cross-Border Privacy Rules (CBPR), however, have gained increasing interest from governments and companies alike because they do not require countries to adjust or change their existing privacy rules. Instead, the CBPR system is a voluntary certification program that allows companies to transfer data between participating economies, ensuring that the certified companies properly protect data while enabling global commerce. These rules are effective because they operate at the company level, through certifications, rather than the governmental level. ITI believes that the CBPR model is forward thinking and holds potential to encourage confidence and trust in the global economic system. As such, ITI asks that the U.S. Government advocate to expand the number of economies participating in the CBPR system.

*Internet-Based Content and Communications Services or Over-The-Top (OTT) Services*

Another disturbing trend is the growth of measures which attempt to unnecessarily regulate internet-based content and communications services, or OTT services. The term "OTT" poses several challenges, as it is overly broad and poorly characterizes the actual role that these services play. These services are an increasingly important element of the broadband value chain and are diverse and fast-evolving, providing solutions that were previously unavailable or unaffordable to many people and businesses. In response to the growth in these offerings, and their disruptive nature to some traditional telecommunications services industries, some countries are seeking to impose ill-fitting or duplicative regulations onto these technologies, without recognizing the meaningful differences between internet-based services and traditional telecommunications services. To complicate the matter, often these regulations are very broad and could be interpreted to cover any services being delivered over the internet. ITI has developed a set of principles to be used in discussion of OTT services. When considering regulating OTT services, policy makers should:

- recognize the meaningful differences in delivery, function, and range of services provided;
- protect the free flow of data to support the growth of the internet ecosystem;
- enable and encourage increased investment in networks;
- avoid regulation except where rooted in legitimate public policy objectives;
- ensure consistency with trade obligations and principles;
- promote global consistency and standardization; and
- enable small and medium enterprises (SME) to compete.

*Harmonization in the development of taxation frameworks*

The growth of the digital economy has demonstrated the need for a consistent global tax regime. Unilateral action by one country to deviate from this regime makes investment decisions harder, cross-border compliance more difficult, market and trade fragmentation more likely, and creates

the potential for costly tax disputes between governments. We urge USTR to work with the U.S. Treasury to monitor tax developments around the world and work towards a more harmonized approach, ensuring that the same dollar of profit will not be taxed twice in two different countries. Together, USTR and the U.S. Treasury should ensure that tax measures do not increase the complexity of cross-border trading in a way that harms market access and the cross-border growth of Internet services.

## Argentina

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 make the SIMI system, which has replaced the DJAI system, not serve as a barrier to trade.

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 manufacture, marketing and business models of the electronic 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. ITI recommends that, instead of city-specific WEEE standards, Argentina create a national WEEE standard to ease unnecessary costs associated with importing into the country.

In December 2009, Argentina increased taxes on various IT products, including mobile phones and cameras, produced outside the Argentine region of Tierra del Fuego. In December 2012, the Government issued Decree 2623, which renews and extends the 2009 tax incentives for local assembly of ICT devices in Tierra del Fuego. Decree 1219 (November 2105) expands these measures, requiring manufacturers to incorporate locally made cables, screws, batteries, chargers, and other accessories and inputs into mobile phones. It also requires companies to prepare a report on the progress of incorporating local components into their production. Discriminatory internal taxes that discourage competition can contribute to the growth of the black and grey markets, increasing risks to consumers, reducing revenue for governments, denying citizens access to the most technologically-advanced devices.

ITI also seeks to ensure that Argentina's regulatory environment does not disadvantage ICT producers with global supply chains that seek international interoperability and global standards. Argentina has recently implemented several regulations for product safety and safety testing, which we urge them to continue to align with global norms. Resolution 75/2016 is intended to allow companies to utilize international certification and safety testing, reducing redundant, expensive, and unnecessary product testing. However, this resolution has yet to be implemented as the Ministry of Production agency *Lealtad Comercial* has not authorized the extension of Mutual Recognition Agreements (MRA). Implementation of this law would greatly improve the ability of U.S. companies to import products to Argentinian market, both improving U.S. exports and providing Argentinians with the most up-to-date products. ITI also encourages Argentina to allow additional international testing and adherence to global standards, especially with regard

to implementation of Resolution 171/2016, which seeks to ensure safety of low power devices.

## Australia

In 2015, Australia passed its Multinationals Anti-Avoidance Law, which appears to be outside the scope of the Organization for Economic Cooperation and Development (OECD) Base Erosion and Profit Sharing (BEPS) recommendations and may impede market access for businesses seeking to serve the Australian market. ITI urges the U.S. Government to engage with counterparts in Australia to develop taxation principles that are consistent with international best practices.

## Brazil

The government of Brazil maintains a variety of 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 8248/91, and Portaria 87/2013); it offers government procurement preferences for local ICT hardware and software (2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903); it requires that federal agencies procure e-mail, file sharing, teleconferencing, and VoIP services from Brazilian "federal public entities" such as SERPRO, Brazil's Federal Data Processing Agency (Presidential Decree 8135 of November 5, 2013 and subsequent Ordinances No. 141 of May 2, 2014, and No. 54 of May 6, 2014), and; it does not recognize the results of conformity assessment procedures performed outside of Brazil (ANATEL Resolution 323). ITI remains interested in the ongoing WTO case against these issues in Brazil, and encourages USTR to continue to ensure that these and new policies in Brazil do not force a local presence, manufacturing or otherwise, as a prerequisite for market access.

Brazil's *de minimis* threshold—for which no duty or tax is charged on imported items 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 to 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 2017 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 in respect to the United States which would allow recognition of testing done in the U.S., easing the time and cost of exporting to the

Brazilian market. Resolution 323 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. Presidential Decree 8135 of November 5, 2013 and subsequent Ordinances (No. 141 of May 2, 2014, and No. 54 of May 6, 2014) required that federal agencies procure e-mail, file sharing, teleconferencing, and VoIP services from Brazilian "federal public entities" such as SERPRO, Brazil's Federal Data Processing Agency. Such measures disrupt the global nature of the ICT industry and disadvantage both access to technology in Brazilian and the ability of U.S. ICT companies to do business in Brazil. In August 2016, the Ministry of Planning announced that Decree 8135 would be revoked. ITI urges Brazil to ensure that any new measures avoid provisions that would hinder Brazilians' access to best-in-class, cloud-based communication services.

In addition, Brazil is currently debating revisions to the legal basis for its telecom sector, and some legislators have supported the idea of regulating online services in a similar way to telecom services. However, this approach risks raising costs for online entrepreneurs and halting Brazil's innovation due to increased bureaucracy and artificial limits on services, harming both local consumers and foreign providers of Internet services. ITI encourages USTR to monitor the development of these legal changes and to engage with Brazilian counterparts to promote a light-touch regulatory framework consistent with the US approach to information services.

Finally, Brazil is considering the adoption of an "adequacy" regime for determining whether data may be transferred to third countries, similar to the model in the European Union. We urge the U.S. government to engage with Brazilian officials to consider less fragile frameworks for ensuring the protection of private data while enabling cross-border information and data flows.

## Canada

Canada's *de minimis* threshold remains at CAD $20 (approximately USD $15), the lowest of any industrialized country and among the lowest in the entire world. For comparison, the *de minimis* threshold for items imported into the United States is $800 USD—over 40 times higher than Canada's. This low threshold, which has not been adjusted since the 1980s, creates an unnecessary barrier to trade through increased transaction costs for Canadian businesses, and acts to restricts consumer choice and competition. Raising the *de minimis* threshold would help Canadian small businesses participate more fully in global trade and ecommerce, growing Canada's economy and enable U.S. small businesses to more easily participate in commerce with Canadian companies and consumers.

## Chile

Chile is regulating the testing and certification for safety and energy efficiency 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.

Additionally, many of these new requirements have been imposed without a regulatory impact assessment or ample consultation with stakeholders. Industry advocates for regulations that allow industry to test their products once at a competent lab anywhere in the world to a single internationally accepted standard. Industry encourages flexibility on the ways to communicate energy efficiency requirements, spectrum compatibility, and emergency alert notifications.

## China

ITI appreciates the work and attention that the U.S. government has dedicated to China and its many discriminatory trade practices, particularly in the area of Intellectual Property Rights (IPR). Strong and balanced IPR protections are of critical importance to the success of high-tech business, as the immense investment into research and development is a necessary for technological development. IPR protections in China have long been a troubled area. U.S. business has continually encountered a lack of IP law enforcement, forced technology transfers, and source code disclosure rules. We request that the U.S. government continue to highlight these problems in China in the 2017 NTE so as to urge China to uphold the international commitments that it agreed to when joining the WTO.

In addition, ITI greatly appreciates the priority the U.S. government has given in raising industry concerns with China's discriminatory cybersecurity regulations. Market access concerns with regard to China's developing framework for cybersecurity regulations continues to be ITI members' priority concern in the China market. The draft Cybersecurity Law, in its current form following the public release of the second draft, creates a legal framework that institutes multiple and overlapping security review regimes for foreign technology that have limited transparency, creating significant opportunity for discrimination under the pretense of cybersecurity. It also creates a framework mandating local analysis of data and mandating security reviews for all important business data to be transferred across China's border. Additionally, ITI members remain extremely concerned with the implications of the China Insurance Regulatory Commission's (CIRC) draft Provisions on Insurance System Informatization, which seem to contain a number of technical barriers to trade, and could institute discriminatory ICT procurement criteria, as well.

Of growing concern to the technology industry—and other industries that depend on ICT platforms for global operations—are requirements to store, process, or manage data locally within China and restrictions on flows of data in and out of China. In particular, there are a raft of laws and regulations that restrict the flow of data relating to the medical (*Population and Healthcare Information Management Measures*), financial (*Notice to Urge Banking Financial Institutions to Protect Personal Information*), credit (*Administrative Regulation on the Credit Information Industry and Credit Reference Agencies*), and online publishing (*Online Publishing Service Management Rules*) sectors. In addition to these, there are broader restrictions requiring explicit permission to transfer data overseas (*Guidelines for Personal Information Protection within Public and Commercial Information Systems*). Two draft measures threaten to further broaden these prohibitions on cross-border data flows: *The Draft Supervision Rules on Insurance Institutions Adopting Digitized Operations* would require local storage of insurance data, and the

*Draft Cyber-Security Law* would require localization of "important" data relating to citizens and critical information infrastructure.

These measures directly affect the ability of many industries beyond the tech sector to conduct normal business operations and represent a dangerous precedent for the control of the internet. This trend toward increased control over where and how data is transferred represents a destructive and misguided attempt to protect Chinese tech companies from foreign competition. Taken together, these measures pose great costs to U.S. firms in all sectors. ITI appreciate that the U.S. government addressed these laws in the 2016 NTE but requests that it give more weight to the harm that specifically the restriction on data flows will cause to U.S. business interests in the 2017 NTE.

Additionally, China's State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) published a notice on the Administration of Publishing Mobile Games for comment in 2016. This regulation restricts the publishing of mobile games to domestic companies. Such a regulation will make it difficult or impossible for foreign app stores to operate in China, given the centrality of mobile games to the growth and popularity of app stores. This notice represents a negative shift from previous steps that China had taken to allow foreign owned app stores to operate through the Shanghai Free Trade Zone. In addition, the scope of this regulation includes platforms such as app stores that have domestically created games within the platform, despite the fact that the platform itself in this situation does not create new material and already manages content in accordance with local law, thus needlessly discriminating against distribution platforms that are not publishers. ITI urges USTR to highlight that these restrictive regulations will create significant market access barriers for foreign service providers, and are contrary to China's existing WTO commitments on computer and related services.

Finally, in China, the world's biggest market, many U.S. services are either blocked or severely restricted. Barriers to digital trade in China continue to present significant challenges to U.S. exporters. This blocking has cost U.S. services billions of dollars as they are 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.

## Colombia

In Colombia, one bill in Congress proposed by the Ministry of Transportation would require online platforms used for the provision of transportation services to register, obtain prior authorization, and provide authorities access to their databases. This proposed law would reduce the ability of innovative companies to effectively do business in Colombia.

The Colombian Ministry of ICTs is evaluating whether or not to extend broadcasting and public utility regulation to streaming platforms, and seeks to propose a bill to reform the TV sector to this effect. A bill in Congress aims at subjecting subscription-based audiovisual streaming platforms to the television public utility legal framework. In addition, there are secondary regulatory initiatives to classify audiovisual streaming services as telecommunications services.

All of these measures constitute unnecessary restrictions on internet based services that would reduce the ability of innovative Colombian internet-based startups to grow and thrive in the Colombian market.

Additionally, there is a tax proposal that would raise VAT tariffs and remove longstanding VAT exemptions, raising barriers for foreign companies in the ICT sector. This initiative seems focused on compelling foreign Internet services and platforms to invest locally. For example, one senator discussing these initiatives noted that many Internet platforms "are not located in Colombia."

As Colombia works to adapt national frameworks to promote the digital economy and innovation, USTR should encourage Colombian policymakers to ensure that technology and innovation can continue to prosper and thrive in Colombia's growing economy, while avoiding the creation of market access barriers that could halt the growth of services that are critical to the economy.

Lastly, there has been a growing trend in Colombia where consultations for regulations are opened with only several days or only one week for comments. These public consultations signal a lack of desire for meaningful input from stakeholders, and go against the WTO and OECD commitments that the country has made regarding trade policy.

## Costa Rica

As stated in the Section 1377 report for the past several years, the Costa Rican telecommunications regulator, Superintendencia de Telecomunicaciones (SUTEL), continues its unique requirement for retesting and recertification of hardware after a software or firmware updates, focusing on certain electromagnetic compatibility (EMC) testing and certification requirements (RCS-092-2011, RCS-431-2010). Such updates are often frequent, and allow users to protect their equipment from security threats and improve their user experience. As a matter of international best practices, many other governments do not require re-testing or re-certification after such updates. These country-specific requirements can also lead to redundant testing, particularly when a product is required to undergo testing to the same standard in both the exporting and importing country. ITI requests that the U.S. government include these measures in the 2017 NTE and address them as soon as possible. ITI believes that they constitute an unnecessary obstacle to trade by delaying updates and imposing burdensome requirements on U.S. software developers while raising costs for consumers in Costa Rica.

## Ecuador

Ecuador adopted RTE INEN 105, which makes compliance with safety, performance or environmental international standards regarding secondary cells and batteries mandatory, including IEC 61960, which is voluntary. All requirements enter into force in December 27, 2016, giving importers and manufacturers too little time to comply. It will severely disrupt trade in secondary cells and batteries, and therefore the ability of companies to support their clients'

needs for replacement batteries. It increases cost and expenses, with no benefit to consumers. In order to obtain the certificate from the Ecuadorian certification entity SAE, the importer of record would need: evidence of compliance with IEC 61960, IEC 62133, US EPA 7471B, and ASTM E536-04a, evidence of compliance with marking requirements, to register as generator of hazardous waste, and to register its operations. While referencing international standards is a sound practice, countries should avoid making voluntary standards mandatory, and in all cases, should provide sufficiently long transition periods for companies to implement the necessary requirements for compliance (including testing, compiling documentation, etc.), which should, in any case, be at least one year. In this example, the lead time for just the test is at least 3 months. ITI requests that the U.S. Government urge the Costa Rican government to adhere to global norms and standards.

## 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.

In particular, in the area of copyright, ITI is concerned that the Commission is considering a set of regulatory measures that would increase market fragmentation, inhibit innovation, and harm market access for US and other foreign services. First, the Commission is considering significantly changing existing principles of "intermediary liability" by requiring online services to create content filtering technology to identify copyright protected material. Second, the European Commission has also proposed the creation of a new "neighboring right," which would give news publishers the right to charge online services a fee when they show even a small amount of news content, such as headlines, on their platforms. Both measures would raise considerable market access barriers for major technology companies, startups, and other entrepreneurs. We provide more information on these measures below.

On the first measure, the Commission has proposed requiring online services to deploy content filtering technologies. This requirement would represent a significant departure by the EU from its shared approach with the United States on the foundational principles of a free and open internet. The Internet is a vibrant and economically valuable platform in large part because of balanced intermediary liability laws, which permit users and small businesses to post material–such as videos, reviews, and pictures–online without being unduly exposed to liability for the content of that material. Both the United States (under Section 512 of the Digital Millennium Copyright Act) and the EU (under Articles 12-15 of the Directive on electronic commerce) create a "safe harbor" that protects online services from being liable for what their users do, as long as the service acts responsibly, such as by taking down content after being given notice that it infringes copyright.

However, the recent proposal by the Commission would significantly deviate from these core principles, by requiring service providers to "take measures . . . to prevent the availability on their services of works or other subject-matter identified by rightholders." This language would create new and unclear filtering obligations that could be implemented in different and inconsistent ways across member states. Service providers would be subject to a moving target in the European Union for years to come. Larger providers would face critical liability risks, while smaller startups and entrepreneurs would likely decline to enter the market, given difficulty of raising funds from venture capitalists that have consistently characterized such rules as strong impediments to investment. Moreover, such filtering technology will be very expensive for large and small services to develop and maintain.

In these ways, this new copyright proposal is quite similar to the "duty of care" that USTR correctly flagged in the 2016 National Trade Estimate as generating numerous market access problems for US-based services, including significant "logistical difficulties," "implications for free expression," and a "regulatory regime to more tightly control platforms' behaviors." ITI encourages USTR to raise even stronger concerns about this new proposal, recognizing that it will serve as a damaging market access barrier for US-based services if it is implemented.

On the second measure, the creation of a new "neighboring right" by the European Commission is similar to failed "ancillary copyright" measures previously introduced in Germany and Spain. This measure would give news publishers additional rights over the usage of even a small amount of news content -- such as a headline or snippet -- on online platforms. Such a measure would be a significant market access barrier for online services. Rather than attempting to navigate complex individual negotiations with publishers in order to include a headline or other small amount of newsworthy content on a third-party site, online services might simply stop showing such content, causing traffic to news publishers to plunge.

Indeed, the response to the introduction of ancillary or neighboring rights in other countries has been catastrophic both for online services—some of which have stopped serving specific EU markets—and for local publishers and news outlets, which have seen strong decreases in the number of daily visitors. As a result, ITI encourages USTR to expand upon its assessment of ancillary copyright and link taxes in the 2017 National Trade Estimate, and classify this proposed measure as a market access barrier.

## India

Of primary concern to the tech industry in India is the Compulsory Registration Order (CRO), which requires manufacturers to submit product samples from each factory for testing by a "BIS recognized laboratory" located in India. Although India is a member of the IECEE CB Scheme, products in scope of the CRO must be tested again, regardless of whether it had already been tested by a member of the CB Scheme. Also, the requirements for registration are incredibly costly to U.S. firms, while providing no better confidence in the safety of the products. ITI requests that the U.S. Government encourages the Government of India to hold consultations with industry and other stakeholders to bring its CRO program into alignment with international

best practices.

In addition, in March 2015, India's telecom regulator, TRAI, issued a consultation paper on "Regulatory Framework for Over-the-top (OTT) services." There has been no response from the regulator on this paper after comments were submitted, yet it appears that the matter is still under consideration. In 2016, there have been additional consultation papers on issues including net neutrality, VoIP, and cloud services. Many of these consultations have sought feedback on whether there is a need for regulation of OTT providers that offer such services. However, again, regulators have provided little feedback or response to industry submissions. Finally, the Ministry of Telecommunications recently released draft registration guidelines for M2M service providers in India, with a focus on increasing regulation of M2M service providers. Given that many of these consultations and drafts could generate restrictive rules and market access barriers for US services seeking entry to the Indian market, ITI encourages the U.S. government to engage with counterparts in India and promote a light-touch regulatory framework for OTT services that is consistent with the principles articulated at the top of this filing.

ITI is also concerned about India's recent vote on an "Equalization levy," aimed at creating an additional 6% withholding tax on foreign online advertising platforms. While this levy was introduced with the ostensible goal of "equalizing the playing field" between resident service providers and non-resident service providers, one significant problem is that its provisions do not provide credit for tax paid in other countries for the service provided in India. Another problem is that this levy will target business income even when a foreign resident does not have a permanent establishment in India—even when underlying activities are not carried out in India—in violation of Articles 5 and 7 of the US-India tax treaty. The current structure of the levy represents a shift from internationally accepted principles, which provide that digital taxation mechanisms should be developed on a multilateral basis in order to prevent double taxation. As it stands, the levy is likely to impede foreign trade and increase the risk of retaliation from other countries where Indian companies are doing business. In addition, there is a risk that the levy will be extended more broadly to cover the full range of foreign e-commerce and digital services. ITI urges the U.S. Government to recognize that this levy may serve as a market access barrier for foreign services, and engage with counterparts in India to develop taxation principles that are consistent with global best practices.

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 number of used equipment and parts shipments. 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. Subsequently, MOEFCC rescinded this Official Memorandum in August. Despite this retrieval, 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 in order 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 threaten to severely restrict future investments in India. ITI requests that the U.S. government include this issue in the 2017 NTE in order to push the government of India to clarify if and how it will enforce this regulation.

ITI remains concerned about the lack of clarity regarding mandatory in-country security testing for ICT products. The Indian government has not published any details or specifics regarding the nature and scope of these testing requirements and ITI is concerned that this testing regime could be a mechanism for forced technology transfer or the inspection of source code and other sensitive IP. While ITI is encouraged by the recent announcement to delay the testing regulations until April 2017, we seek greater certainty than year-long extensions can provide. Specifically, we urge the U.S. Government to engage the Indian Department of Telecommunications to gain assurances that there will be sufficient implementation periods provided of at least 9-12 months. This 9-12 month implementation period should begin only after all consultations have occurred, rules have been finalized, and guidance on any implementing documents been provided. ITI continues to recommend that the Indian government align its approach with global best practices to assure the cybersecurity resiliency of telecommunications networks, which include reliance on industry-driven and consensus-based technical standards and best practices as well as the acceptance of testing and certification results based on international standards from internationally-accredited labs.

Finally, ITI continues to be concerned with the government's efforts to implement the Preferential Market Access policy for government procurement (PMA-G). While ITI understands the desire to promote domestic manufacturing, we believe there is a way to do so without mandating preferences for domestic players. Of significant concern, the GOI recently announced that PMA-G would apply to high-end systems, such as servers and storage equipment, but should focus on mass-produced, consumer electronic products. This requirement is extremely problematic given the lack of an advanced manufacturing ecosystem in India. If implemented, ITI member companies would be unable to compete fairly for government ICT contracts.

## Indonesia

The government of Indonesia has increasingly introduced forced localization measures into its trading regime in order to favor local companies at the expense of foreign competitors. First, the Ministry of Communication and Informatics (MICT) Regulation 82/2012 continues to be a primary concern for the tech industry. This law contains data center and disaster recovery center localization requirements and source code surrender for software developers, along with other onerous requirements that would impose large costs on all U.S. industry sectors that wish to do business in Indonesia. Though it appears that an amendment to this law is being considered, there are no details forthcoming on the nature and extent of the amendment. This regulation warrants continued attention and focus from the U.S. Government in the 2017 NTE.

Indonesia's new Patent Law also contains "localization" rules that require foreign patent holders to transfer proprietary technologies to local companies. The patent holder is obligated to make the product or use the process in the territory of Indonesia and there is no exception for this provision.

In addition, Regulation 27/2015, *Technical Requirements of Equipment and Telecommunication Devices Standards-based of Long Term Evolution (LTE) Technology*—in addition to a more recent regulation, Regulation 65/2016—impose 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 would roll 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. ITI requests that the U.S. government include these regulations in the 2017 NTE and address them as soon possible, as they impose significant barriers to trade for U.S. phone hardware manufacturers. 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.

Lastly, 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. The 2017 NTE should address this measure and its potential damages.

In addition, Indonesia has taken steps on taxation that significantly deviate from global norms, bilateral tax treaties, and WTO commitments. These steps include proposed requirements that would compel foreign services to create a permanent establishment in order to do business in Indonesia. For example, Article 4 of the draft regulation described above requires providers to create a local entity or permanent establishment, as well as undergo a rigorous process of registration, including first with the IT regulator (BRTI) and then with BKPM in order to establish a business entity. This process would require significant resources from online service providers, many of which are small companies that lack the necessary legal and technical resources to comply with such processes, and could have significant tax consequences that conflict with OECD multilateral principles. Furthermore, this requirement would likely violate Indonesia's WTO commitments to allow computer and other services to be provided on a cross-border basis. ITI urges the U.S. Government to classify these disproportionate taxation measures as market access barriers.

## 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 US approach.

In addition, we urge the U.S. government to monitor new developments regarding data localization in Kenya, and engage with counterparts in the Kenyan government on recent draft legislation that may include ambiguous localization requirements.

## Malaysia

In Malaysia, there has been a proposal to include regulation of online services within the jurisdiction of communications regulators. In addition, last year, the Malaysian Communications and Multimedia Commission (MCMC) decided to assess the need for improvements to the Communications and Multimedia Act (CMA). ITI encourages the U.S. government to monitor the development of these regulatory frameworks and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach. In particular, Malaysia should avoid creating market access barriers by subjecting foreign Internet services and applications to telecom-specific or public utility regulations.

## Mexico

In 2014, Mexico's National Commission on Efficient Energy Use (CONUEE) had two energy efficiency measures, NOM-032 and NOM-29, which require certain testing methods, standby energy consumption limits, and labeling for electronic and electrical equipment. These labeling requirements not only have little to no benefit to the Mexican consumer, but also add large costs to ICT producers. This overly trade restrictive measure warrants continued attention from the U.S. government in the 2017 NTE.

Additionally, the Mexican federal government has delegated WEEE standards to the states. The result is that companies operating across the country encounter differing and often inconsistent rules for labeling products, requiring them to change labels and markers as those products move from one state to the next. This is unnecessarily burdensome for importers and should be addressed at the federal level.

On April 20, 2015, Mexico's tax authority, the Servicio de Administración Tributaria (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 imports cumbersome and sometimes impossible, as it asks for documents that are non-existent, confidential, or issued after the import. SAT has twice delayed the enforcement of this requirement. 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 the U.S. government include this this issue in the NTE 2017 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.

Mexico's Customs Agency seeks to modify the simplified imports model via couriers (amendments to the current Foreign Trade Rule 3.7.3. and proposed new Rule 3.7.35) by increasing the VAT and duty for express shipments, in addition to several new requirements, such as reporting the HS code of every product contained in an express shipment and monthly reports listing tax IDs for customers and shipment invoices. Mexican authorities should avoid the implementation of excessive measures that will transform the courier model into something similar to the definite imports model, eliminating the simplified procedures and hurting Mexican e-commerce, small and medium businesses, and consumers in general. Maintaining a simplified imports model not only helps fuel the growth of a new sector of the Mexican economy, but also brings consumer benefits by allowing wider selection of products at the best possible prices. Mexican Customs authorities should 1) to ensure compliance with its national and international and commitments regarding foreign trade facilitation, as expressed in the TPP and the TFA—to which Mexico recently adhered; and 3) evaluate the alternate rule proposed by courier companies. Industry requests the U.S. government include this issue in the NTE 2017 and immediately oppose these changes.

ITI encourages USTR to ensure Mexico upholds data flow commitments that it agreed to under the TPP. In the coming year, the Mexican Congress will make changes to data policies in two separate pieces of legislation: 1) the draft law on data held by the public sector, and 2) the draft law on data held by the private sector. These upcoming bills are an opportunity for resolving uncertainties regarding cloud services and crafting positive data privacy models. ITI would welcome USTR's review of both data privacy bills.

## Panama

Panama has introduced a new Data Protection bill. ITI members are troubled by the fact that this bill does not appear to recognize consent as a basis for transferring data outside the country. Any international transfer provision should permit transfers with the consent of the data subject, and the nature of that consent (e.g., whether it is express or implied, and the mechanism used to obtain it) should be based on the context of the interaction between the controller and the individual and the sensitivity of the data at issue. The required consent for transfers should not

be burdensome, and should allow for the use of technology-neutral consent approaches. In addition, consent should be implied for common use practices such as transferring data to cloud computing service providers located abroad. We encourage USTR to engage with counterparts in Panama to develop interoperable data protection frameworks that clearly allow for the forms of consent described above.

In addition, Article 2 of the Data Protection bill mentions that databases containing "critical State data shall be kept in Panama." The definition of critical State data set forth in Article 3 is, however, very broad. This could create a *de facto* data localization mandate for all data, even if this is not the objective of the law. The U.S. government should work with Panama to ensure that this language does not result in a broad data localization requirement.

## 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 of their data concerning Nigerian citizens in Nigeria. It also establishes 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. This explicit localization regulation will cause economic damage for businesses across all sectors in Nigeria—an increasingly important market. These rules would 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 2017 NTE and continue to monitor the development of this policy closely.

## Philippines

In September 2014, the government released a draft administrative order that appears to require government agencies to procure cloud services from the Government Cloud, and only where this is not possible will they be permitted to purchase commercial cloud services. These restrictions could prevent Philippine government agencies from accessing best-in-class cloud services. This is further aggravated by government procurement preferences that generally favor local companies and locally produced materials and supplies.

In addition, telecommunications regulators have sometimes interpreted existing regulations to mean that cloud service providers are required to obtain a Valued Added Telecom Services license, which is open only to Filipino companies. The requirement has not been consistently enforced, but if it were, it could severely limit overseas companies' ability to provide cloud services in the Philippines.

## 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. ITI requests that the U.S. government continues 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 closely monitors the development of this plan and highlight its potentially discriminatory elements in the 2017 NTE.

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.

Lastly, on July 7th, 2016 President Putin signed a package 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 have to 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.

## Saudi Arabia

In July, 2016 the Communications and Information Technology Council (CITC) issued the *Public Consultation Document on the Proposed Regulation for Cloud Computing*. This thoughtful and well-structured consultation signals a positive development in the Kingdom's notice and comment practices. The proposed regulation has several troubling provisions—including tiered licensing requirements, data localization requirements for certain types of data, and potentially un-workable provisions on data protection—which ITI and its member noted in their comments, and which may be rectified. ITI requests that the U.S. Government watch developments around this potential regulation as it develops throughout the year.

## Senegal

In Senegal, the Regulatory Authority for Telecommunications and Post (ARTP) has publicly announced a study to help decide whether and how to regulate OTT services. ITI encourages the U.S. government to monitor this study and to promote a light-touch framework for regulating information services that promotes market access for foreign services.

## South Africa

South Africa is reviewing draft changes to its intellectual property policy. It is important that any such changes support balanced intellectual property protections for software and other information and communication technologies that foster innovation and growth.

## South Korea

The Cloud Computing Promotion Act was passed in 2015 but significant barriers still exist to the adoption of public cloud services, especially those that are provided from offshore locations. Under government procurement policies, all public sector agencies are required: (a) to ensure that server, network, security equipment they procure are physically separated from cloud computing services consumed by general users; and (b) ensure that only specific encryption algorithms that are recognized locally are used in IT products that incorporate encryption

technology. These government policies effectively favor local IT providers to the detriment of foreign service providers. Furthermore, in the healthcare sector, medical records must remain onshore and backup systems need to be physically segregated from other systems that process patient data.

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 go against international standards for global interoperability of payments technology. Using local instead of international standards would lead to lower levels of investment and innovation in payments in Korea and would depress consumer spending in the cross-border travel and tourism sectors.

## Turkey

In 2014 Turkey passed the E-Payment Law, requiring companies to process all digital payment transactions initiated in Turkey in a data centers within Turkey's borders. This data localization requirement acts as a high barrier for entry into the Turkish market for SMEs and impacts the operations of all companies in Turkey whether foreign or domestic. The costs have been so high, in fact, that prominent U.S. e-payment companies have considered exiting the market all together. 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 2017 NTE, appropriately reflecting the economic impact it has on companies operating in Turkey.

## 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 have continued 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.

## Uruguay

Uruguay is currently considering a bill to regulate digital platforms and services. However, this draft bill is vague and broad, and could affect a wide range of Internet services and products. ITI

encourages USTR to monitor the development of this bill and advocate for consistency with the principles for regulation of OTT services provided within this filing.

## Vietnam

Vietnam has increasingly considered or implemented restrictive forced localization measures. First among them is the *Decree on Information Technology Services* (Decree No.72/2013/ND-CP). This law requires every digital service or website to locate and least one server within Vietnam. Clearly 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 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 it in the 2017 NTE, and continue to work with Vietnam in reconciling this law with its future Trans-Pacific Partnership (TPP) obligations.

Vietnam's Ministry of Information and Communications recently introduced a new draft decree (Draft Decree Amending Decree 72/2013-ND-CP) 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 would 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, Section 512 of the DMCA, and Article 18.82 of the TPP.

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 US 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 addition, Vietnam's *Law on Network Information Security* (LONIS) contains multiple troubling provisions in regards to 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. This law imposes large costs on U.S. industry and appears to be inconsistent with Vietnam's future TPP obligations.

As mentioned in the 2015 NTE, the government of Vietnam also promulgated a draft IT Services Decree that would have included additional data localization requirements as well as restrictions on cross-border data flows. While the government of Vietnam later shelved the draft decree, ITI has heard indications that it is now being reconsidered. 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. In particular, 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 unless they enter into a commercial agreement with local telecommunications companies.