CompTIA

October 31, 2019

Written Comments to the Office of the United States Trade Representative for the National Trade Estimate Report on Foreign Trade Barriers

(USTR-2019-0012)

The Computing Technology Industry Association (CompTIA), the leading association for the global information technology (IT) industry, welcomes this opportunity to provide the following comments to the Office of the United States Trade Representative (USTR) and the Trade Policy Staff Committee (TPSC) for inclusion in the National Trade Estimate Report on Foreign Trade barriers (NTE). CompTIA is providing these comments in response to USTR's Request for Public Comments to Compile the National Trade Estimate Report on Foreign Trade Barriers via docket number USTR-2019-0012. Below, is a series of summaries of technological trade impediments to the major trading partners of the United States including Argentina, Austria, Brazil, China, Dominican Republic, European Union, France, Germany, India, Indonesia, Japan, Korea, Nigeria, Philippines, Saudi Arabia, Thailand, Turkey, and Vietnam.

Argentina

Telecommunications, Communication and Information Services

Argentina continues to be a major trading partner with the United States, especially since the establishment of the 1991 bilateral investment treaty. Despite this however, there remains specific barriers to trade, particularly with cross-border data flows in the telecommunications, communications, and information services sectors. The Argentine Ministry of Modernization drafted a new Convergent Communications Law which covers the rights and obligations of users of ICT services. There are concerns that the scope of the proposed regulations could be too broadly interpreted to create rights for users of all ICT services. Argentina should limit the scope of the obligations to consumer-facing, regulated telecommunications services. New services, such as the internet of things and over-the-top (OTT) applications, should also be exempted from these consumer rights obligations because they fall outside the scope of regulated telecommunications services.

Austria

Digital Ads Tax

The Austrian Digital Ads Tax was approved in Austria's Budget Committee on September 12, 2019 and Austria's Federal Council on October 10, 2019. The 5% tax will go into effect on January 1, 2020 with collection due later in the year. CompTIA is highly concerned with the discriminatory nature of the tax, specifically against successful American digital companies. The tax will be applied to any company with 750 million euros ($826 million) in worldwide revenue and 25 million euros of digital advertising revenue in Austria. CompTIA members are also concerned about the digital tax proposals and actions in France, Italy, Spain, the UK and others. CompTIA endorses the ongoing negotiations at the OECD, as a multilateral solution to

appropriately taxing the digital economy is far superior to a unilateral tax that seeks to unfairly encumber successful American technology companies.

Brazil

Local Content Requirements for Information and Communication Technology Products

Brazil is another major United States trading partner which continues to create barriers to investment, particularly by implementing local content requirements for ICT products. Brazil has adopted a slew of policies over the years that require the use of local content for its government procurement in ICT. Brazil's *Basic Production Process* requires a minimum level of local content and procurement preferences in the ICT sector. Brazil's measure was challenged at the WTO with the dispute settlement panel finding some aspects of the measures to be inconsistent with Brazil's WTO obligations.[1]

China

Tariff Charges

China is one of the United States largest trading partners; however, China continues to implement aggressive trade barriers to technology sector by imposing tariffs directly against the World Trade Organization's (WTO) Information Agreement (ITA). The ITA was negotiated in December 1996 and led to the elimination of import duties on numerous high-tech products which in 2013, accounted for an estimated value of $1.6 trillion. The original ITA covers 82 WTO members and in July 2016, WTO members expanded the list of covered products to include newly invented technology products. This expansion of the ITA, eliminated tariffs on an additional list of 201 products and covers new generation semiconductors, semiconductor manufacturing equipment, GPS navigation equipment, and medical equipment. The agreement also contains commitments to tackle non-tariff regulatory barriers in the IT sector, and to conduct ongoing reviews of covered products to determine whether further changes are required given the pace of technological developments.[2]

China is a member of the original ITA and the ITA expansion agreement. China agreed to eliminate tariffs via an equal, annual tariff cut over a five-year period commencing on September 15, 2016. However, when the 2017 Harmonized Tariff Schedule went into effect on January 1, 2017, China reclassified 17 semiconductor products thus, putting new import tariffs of 3.2% or 3.4% on previously ITA duty-free semiconductor products. The intention of the ITA and ITA expansion is to eliminate tariffs. This action is a direct violation of that intention.

Cross-Border Data Flows

Additionally, CompTIA members continue to have issues with China's restriction of the free flow of data across borders. Policies invoking "forced data localization" measures require

[1] Panel Report, Brazil - Taxation (Japan) (under appeal).

[2] Please see https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm.

require technology service providers to process and store data domestically based on national security or data privacy concerns. These measures reduce the competitiveness of U.S. companies in China by restricting their ability to store and process data, regardless of location, and increase the costs of doing business in foreign markets due to the need to develop local data centers and infrastructure.

China's Cybersecurity Law (CSL), enacted in June 2017, is just one of the policies that reflect a national security regime aimed at marginalizing the U.S. technology sector. China houses several sector-specific regulations prohibiting the transfer of certain types of data outside of China yet, the CSL specifically imposes restrictions on the cross-border flow of data and data localization requirements regardless of industries. CSL Article 37 states that "personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." Concerns include that Chinese authorities can interpret this law as providing expansive access to private information, trade secrets, intellectual property, or internal business communications.[3]

Local Testing and Certification of Information Communications Technology (ICT) Products

In addition to restrictions of data flows as outlined in China's CSL, CompTIA members have concerns of trade barriers through unreasonable local testing and certification requirements of certain ICT products. These requirements often depart from international standards and result in increased costs for U.S. companies operating in these markets. China's Cybersecurity Law, Encryption Law, and associated regulations require certain ICT products and services to pass an intrusive cybersecurity review or undergo a burdensome licensing regime that may require disclosure of source code or other sensitive and proprietary information.

A. **Cybersecurity Classified Protection Scheme (CCPS):** On June 27, 2018, China officially established a cybersecurity protection baseline for network operators and a universal compliance framework for the CSL by releasing the draft Cybersecurity Classified Protection Scheme Regulation (Draft CCPS Regulation)[4], a continuation of the Multi-level Protection Scheme (MLPS) jointly established by MPS, the State Encryption Management Bureau (SEMB), the Ministry of State Security (MSS), and the State Council Information Office (SCIO) in 2007. Like MLPS, CCPS ranks the importance of network and information systems on the basis of their importance to China's national security, social order, public interests, and the legitimate interests of individuals and organizations on a scale from 1 to 5, with Level 5 constituting the most sensitive to national security interests. Among the most concerning elements is the stipulation that all products or services that could potentially impact national security must pass a "national security review" conducted by the CAC in collaboration with other departments. The contents and procedural process of this

[3] Congressional Research Service, China-U.S. Trade Issues, August 2017

[4] Cybersecurity Classified Protection Scheme Regulation (Draft for Comment) (June 27, 2018), http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html.

national security review have yet to be specified, leading to worries of IP and data privacy protection and discrimination in favor of domestic products.

B. **Cybersecurity Review Regime:** In May 2017, the Cyberspace Administration of China (CAC) officially released the Interim Security Review Measures for Cyber Products and Services,[5] which have been under preparation since 2014. The review examines important ICT components, cyber products, and services procured for use in networks and information systems related to national security and focuses on the "security and controllability" of the product or service. Under this regime, the Cybersecurity Review Office, an office created for this purpose within the CAC Cybersecurity Bureau, will decide whether to review a product or service at the request of a relevant state department, a national industry association or based on public feedback from users. Industry regulators in finance, telecommunications, energy and transportation will conduct cybersecurity review work in their respective sectors. If a cyber product or service fails to pass the cybersecurity review, it will be barred from CII procurement. This regime goes against China's WTO commitment to an open market and global trade. It also creates adverse negative effects for foreign investors in the China market, as well as for Chinese consumers who could be blocked from purchasing certain ICT products.

C. **Cyber Critical Equipment and Cybersecurity Specific Product Catalogue:** The Catalogue of Network (Cyber) Critical Equipment and Cybersecurity-Specific Products (Batch 1)[6] jointly was released on June 9, 2017, with retroactive effect from June 1, 2017, without a comment period or consultation with industry. The Catalogue introduces a market-entry requirement for the listed equipment and products, mandating that they be certified or tested in accordance with relevant national standards before entering the market. The Catalogue requires that testing conform to Chinese standards and "other mandatory requirements," which remain unspecified. The Catalogue includes products that have not previously faced mandatory market access requirements, including routers, switches, servers and programmable logic controller equipment. The Catalogue constitutes a technical regulation as defined by Annex 1 of the WTO Technical Barriers to Trade (TBT) Agreement. All draft technical regulations that are not based on, or deviate from, relevant international standards and have a significant effect on cross-border trade must be notified to the WTO secretariat as early as possible at a time when amendments can still be introduced and considered. However, China failed to notify WTO TBT Committee of the Catalogue and did not allow an opportunity for interested parties to comment.

[5] The Chinese text and unofficial translation of the measures are available at: https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/.

[6] Catalogue of Network (Cyber) Critical Equipment and Cybersecurity-Specific Products (Batch 1) (June 9, 2017), http://www.cac.gov.cn/2017-06/09/c_1121113591.htm.

D. **Draft Cryptography Law:** The latest Draft Cryptography Law, with comments ending in September 2019, is China's first law governing cryptography.[7] While core and common cryptography are related to state secrets and are off limits to foreign participation, commercial cryptography is partly open for foreign participation. Overall, the draft Law adopts a broad regulatory approach towards commercial cryptography, which is counter to the global nature of ICT products and services and appears to be inconsistent with China's 1999 "core function" test commitment and commitment to observe the World Semiconductor Council (WSC) encryption principles. Under its WSC commitment, the Chinese Government agreed to not restrict market access to commercial ICT products which implement commercial encryption. The draft Law imposes a unique licensing scheme for the sale, use, import and export of commercial cryptography without clearly defining the scope. For the purposes of the draft Law and implementing regulations, a "core-function commercial cryptographic product" should be defined as a product where encryption is its core or main function, rather than an ancillary feature of the product or one of its components. The licensing obligations that apply to these products should be different from those that apply to core or common cryptography. Because encryption is a standard feature of almost all technology products, the draft Cryptography Law could significantly affect the importation, sale and use of commercial ICT products developed by our member companies.

E. **Internet Security Supervision and Inspection Provisions:** On September 30, 2018, the Ministry of Public Security (MPS) released final Internet Security Supervision and Inspection Provisions by Public Security Organs with an effective date of November 1, 2018. The Provisions derive authority from China's Cybersecurity Law (CSL), Anti-Terrorism Law (ATL), *and* Police Law, and authorize Public Security Organs (PSOs) with broad power to conduct on-site inspections or remote testing on Internet service providers (ISPs) and network-using units to check basic compliance with CSL, ATL and other cybersecurity related laws and regulations. Industry concerns include access to companies' networks, broad and unclear scope, and lack of advance notification, transparency, due process or clear recourse processes.

Telecommunications, Communication and Information Services

U.S. tech companies are also concerned about the Expansion of Telecom Services Regulations and the Communication and Information Services Regulations in China.

A. **Expansion of Telecom Services Regulations:** In March 2016, a new Telecommunications Services Classification Catalog went into effect,[8] expanding the scope of China's telecoms regulation and imposing a host of associated market access restrictions on foreign firms in activities not typically regulated as telecom in the rest

[7] "Releases China Updated Draft Encryption Law for Public Comment," (July 2019). Covington & Burling LLP: https://www.insideprivacy.com/data-security/cybersecurity/china-releases-updated-draft-encryption-law-for-public-comment/

[8] Notice of the Ministry of Industry and Information Technology on the issuance of the Catalogue of Telecommunications Services (2015 Edition) (Dec. 28, 2015), http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c4564595/content.html.

of the world. The measures incorrectly classify a wide range of ICT technologies and services as telecom value-added services, when in fact they are computer or business services that utilize the public telecom network as a method of delivery. For example, the catalogue classified cloud computing, content delivery networks and online interactive platforms (called information services) as telecommunications services. Foreign firms that provide value-added services in China can only operate through joint ventures, of which they may own no more than 50 percent. In short, because of the update, foreign firms that provide a range of ICT services are now subject to explicit market access limitations, and indirectly, mandatory technology transfer to the local partners of joint ventures.

B. **Communication and Information Services Regulations:** The protection of the rights of value-added service (VAS) providers in China's market is insufficient. In addition to the restrictions on market access described above, it is critical for VAS providers to have access to basic telecommunications network elements on reasonable terms and on a non-discriminatory basis. Considering the limited competition in China's market and the fact that its three principal carriers are state-owned, the Chinese government has an important responsibility to ensure adherence to the principles laid out in the General Agreement on Trade in Services (GATS) Annex on Telecommunications. In addition to the market access restrictions on new services created by China's expansive Telecommunications Services Catalogue, China imposes even greater restrictions on any entity seeking to provide traditional, or "basic," telecommunications services in China. To obtain a license to provide basic telecommunications services, a foreign company must enter into a partnership with one of China's State-Owned incumbent carriers, limit its investment to 49 percent equity, and obtain approval from the Ministry of Industry Information Technology (MIIT).

   Additionally, China imposes unreasonably high capitalization requirements for basic telecommunications services. Basic services licenses are subject to a $163 million joint venture capitalization requirement, 100 times larger than the joint venture capital requirement for China's VAS licensees. This is an excessively burdensome restriction that violates Article VI of the GATS. China has already established a precedent for lowering its foreign joint venture capitalization thresholds in other sectors, including insurance and trading companies, and it should now remove this barrier to market access in the telecom sector.

   Furthermore, China has not implemented its WTO Reference Paper commitment to establish an independent regulator. The Chinese government still owns and controls all major operators in the telecommunications industry, and the MIIT still regulates the sector. China should establish a regulatory body that is separate from, and not accountable to, any basic telecoms supplier. This body should be capable of issuing impartial telecom decisions and rules.

Local Content Requirements for Information and Communication Technology Products

CompTIA members are also concerned with countries that have enacted measures that force U.S. companies to use domestic information and communication technology (ICT) products. These measures restrict trade and inhibit choice and innovation. China's Cybersecurity Law (CSL) appears to promote the development of local technologies and impose restrictions on foreign firms. For example, CSL Article 15 directs government entities to "support key network security technology industries and programs; support network security technology research and development, application and popularization; spread safe and trustworthy network products and services; protect the intellectual property rights for network technologies; and support research and development institutions, schools of higher learning, and so forth to participate in State network security technology innovation programs."[9]

Intellectual Property Rights

Intellectual property, such as source code, is the crown jewel of many U.S. technology companies, with U.S. licensing revenues alone totaling over $112.5 billion in 2012. As of 2014, IP-intensive industries supported 45.48 million jobs in the United States, about 30 percent of all employment. In 2018, the U.S. Trade Representative claimed that IP theft by Chinese entities costs the U.S. between $225 billion to $600 billion annually, consistent with the number reported by the Commission on Theft of American Intellectual Property in 2017.[10]

Patents and Licensing: The U.S. ICT sector continues to be concerned about Chinese government interference in licensing agreements. The Chinese government has publicly articulated a policy to promote the domestic development of essential IP. China seeks to foster the domestic development of innovative technologies and IPR in part through technology mandates or promotion of unique national standards that are then turned into technical regulations. Such interference is a departure from how business is conducted and how technology transfer arrangements are concluded in the global market.

A. **Enforcement:** Enforcement actions should be measured against China's commitments under the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) to provide copyright owners with "effective action against any act of infringement in intellectual property rights covered under this Agreement" (Article 41) and if the infringement amounts to "willful trademark counterfeiting or copyright piracy on a commercial scale" to provide for criminal penalties including imprisonment and monetary fines sufficient to provide a deterrent to future acts of piracy (Article 61). Though there have been several positive IP enforcement developments, effective criminal or civil enforcement remains wholly inadequate and unreliable.

B. **Trade Secrets:** China does not currently have a standalone trade secrets law, and trade secrets remain one of the most at-risk types of IP for multinational companies in China. Article 39 of TRIPS states that members shall protect "undisclosed information" and "data submitted to governments or governmental agencies" using

[9] Congressional Research Service, China-U.S. Trade Issues, August 2017

[10] "How much the US lost from China's IP theft?" (March 2018). CNN: https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html

effective measures. To fulfill commitments to trade secrets protection and enforcement, China should follow the Best Practices in Trade Secret Protection and Enforcement Against Misappropriation as adopted by the Asia-Pacific Economic Cooperation (APEC) and develop a comprehensive trade secrets law.

C. **Counterfeit Semiconductors:** Data suggests that China is a major source of counterfeit semiconductors that undermine the quality and reliability of electronics products both inside and outside of China. China's General Administration of Customs (GAC) and other law enforcement and market surveillance agencies should encourage the seizure of counterfeit products and take actions leading to the arrest of counterfeiters and counterfeit traders.

D. **Standards in China:** China is aggressively implementing and utilizing technical standards to support development of key domestic industries, especially in the ICT industry. Challenges for ICT companies include China's development of local standards that aim to displace global standards when mandated. Local standards create significant interoperability issues because they possess important diversions from global standards, lack enough safeguards to protect the intellectual property at issue in standards-setting activities and are developed without adequate transparency and participation rights for foreign companies. Furthermore, voluntary standards often are made mandatory through various administrative measures, and without enough notice to foreign companies. In addition, the implementation of 'voluntary' standards as 'mandatory' standards, oftentimes through the conformity assessment process, is a significant impediment for U.S. companies' growth in the China market. These barriers continue to impede innovation by restricting both the ability of Chinese companies to serve other markets as well as foreign companies to serve domestic markets.

E. **Cloud Services in China:** Cloud computing, despite being identified as an area of strategic development in China, remains largely off limits to foreign companies. Further, draft Chinese regulations, combined with existing Chinese laws, if implemented would force U.S. cloud service providers to transfer valuable U.S. intellectual property, surrender use of their brand names, and hand over operation and control of their business to a Chinese company to operate in China.

Dominican Republic

Telecommunications, Communication and Information Services

In May 2017, the Dominican Republic's Chamber of Deputies approved a tax of US$0.02 on international voice minutes to finance the expansion of its 911 national emergency system. The fixed tax is to be paid by all operators registered with the Dominican Telecommunications Institute (Indotel) and is assessed per minute of international voice traffic. A tax of USD 0.0025 is also payable for each international SMS received by the operators. The Dominican Republic's high termination rates are not in accordance with its obligations under the WTO or the Central American Free Trade Agreement (CAFTA), which requires that the provision of interconnection services by major suppliers be at cost-oriented rates. Further, the discriminatory application of the tax to only

international traffic places the cost burden to build out the national 911 system on foreign consumers, rather than on the domestic consumers who will benefit from this new service.

European Union

Discriminatory Digital Taxation Measures

CompTIA members are deeply concerned at the rise of unilateral and discriminatory digital taxation measures from the European Union, many of which are explicitly targeted at U.S. technology firms. EU member states including Austria, France, Italy, Spain, the United Kingdom and others have sought to get out in front of the OECD by proposing taxes that are linked to local users of U.S. search engines, social media platforms, and online marketplaces, in violation of international tax standards and double taxation treaties as well as the GATS. CompTIA supports the United States' continued leadership in and support of the OECD's work that would reform international tax rules for digital companies that are heavily reliant on intangible assets. We encourage the U.S. government to continue working against digital taxation measures in favor of finding a more equitable, holistic, and fair taxation solution.

Telecommunications, Communication and Information Services

In 2017, the EU Office of Communications (OFCOM) published two consultations for comment – the Narrowband Market Review and the Mobile Call Termination Review. In both consultations, OFCOM proposes not to allow UK operators to apply differential termination charges for calls originating outside the EU/EEA but instead to require them to apply the same termination rate to all calls regardless of the country of origin. This is a positive development because CompTIA member companies to continue to see EU-based operators charge higher rates for terminating calls originating outside the EU than those charged for calls originating inside the EU.

EU Customs Classification of Technology Products

CompTIA members are also concerned with current EU laws regulating the customs classification of technology products. As it currently stands, the EU does not administer its customs laws through a single customs administration. As a result, each of the 28 member states may administer customs laws differently. This system creates unnecessary burdens for U.S. companies that sell technology products in the EU due to inconsistencies across EU Member States and inadequate procedures for companies trading in technology products to challenge customs matters in administrative actions.

France

Digital Services Tax

CompTIA is highly concerned with the French Digital Services Tax (DST) that the French Parliament approved in 2019 and is retroactive to January 1, 2019. The DST is discriminatory nature, specifically against successful American digital companies. Due to the income requirements of the tax, roughly thirty companies would be impacted by the DST. While the likely list of taxpayers includes firms from other countries, the tax requirements

disproportionately harm some of the most successful global enterprises based in the U.S. CompTIA endorses the ongoing negotiations at the OECD, as a multilateral solution to appropriately taxing the digital economy is far superior to a unilateral tax that seeks to unfairly encumber successful technology companies.

Germany

Cross-Border Data Flows

U.S. companies continue to be concerned about data localization requirements proposed by the German government. On November 23, 2017, a new national regulation entered into force requiring machines with a non-German telephone country code to register with the German telecommunications regulator (Bundesnetzagentur, aka BNetzA) to communicate automatically to other machines via the telephone network if located permanently in Germany.[11] For U.S. companies providing global machine to machine (M2M) and Internet-of-Things (IoT) services, this presents a challenge to comply as the behavior of permanent or occasional location of the consumer is unknown.

Telecommunications, Communication and Information Services

On June 28, 2017, the German telecommunications regulator (Bundesnetzagentur, BNetzA) suspended enforcement of a provision of the German Telecommunications Act following a court ruling that the implementation of the German data retention requirement was incompliant with European law. The provisions would have required providers of publicly available telephone services for end users and providers of publicly available internet access services for end users to retain certain metadata (number of the calling and called party, date and time of the connection, etc.) from July 1, 2017, onwards. While the law is not enforced, it remains in effect. U.S. companies continue to be concerned about another aspect of the law that requires providers of publicly available telecommunication services to store the respective data locally within Germany. This data localization requirement will likely not be part of the court's full review. U.S. market participants in Germany invested to upgrade their systems – with investments being non-recoverable – to ensure continued legal compliance.

India

Tariff Charges

On July 1, 2017, the Government of India imposed a Basic Customs Duty (BCD) on mobile phones and ink cartridges imported into India, bringing the duty from zero to 10 percent to which later increased to 20 percent in 2018.[12] India has stated that the duty will backfill the tax

[11] Numbering plan for mobile numbers, consolidated version applicable as from 23 November 2017 (Administrative Order No 11/2011, Official Gazette No 04/2011 of 23 February 2011, amended by Administrative Order No 36/2013, Official Gazette No 14/2013 of 31 July 2013, Administrative Order No 43/2013, Official Gazette No 17/2013 and Administrative Order No 78/2017, Official Gazette No 16/2017 of 23 August 2017) (Nov. 23, 2017), https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/NumberManagement/M2M/M2MCommunications.pdf

[12] "Customs duty raised on telecom equipment." (October 12, 2018). The Economic Times: https://economictimes.indiatimes.com/news/economy/policy/customs-duty-raised-on-telecom-equipment/articleshow/66173069.cms

and protect its industry from foreign competition. India's action to impose this tax is in violation of its binding WTO commitments, and ITA commitments. This action is part of a larger systemic problem that must be addressed.

India has been a member of the Informational Technology Agreement (ITA) since 1997. Despite this, however, India has implemented a protectionist campaign to lessen telecom equipment imports, adversely affecting the U.S. telecom sector. In October 2018, New Delhi announced that it will go against their ITA commitments and impose significant duty increases on numerous telecom products. India continues to levy tariffs on ICT goods since July 2017, insisting that these tariffs were not placed on products that captured by the ITA as IT technology has evolved over the past decades. India's national telecom regulator also announced that it will cut imports of telecom equipment to a "net zero" by 2022. These actions make American products more expensive and less competitive in the Indian marketplace.

Cross-Border Data Flows

In July 2018, India released a draft Personal Data Protection Bill developed by the Committee of Experts on Data Protection which is currently under consideration by the Ministry of Electronics and Information Technology. Several provisions of the draft bill could present compliance concerns for U.S. companies. The draft bill should provide greater flexibility for the processing of personal data; should not mandate the storage of personal data in India; and should provide more flexible mechanisms for cross-border transfers of personal data. Key definitions should also be clarified. Further, provisions on enforcement and penalties are disproportionate and create unpredictability. The Bill gives discretionary powers to local Data Protection Authority (DPA) to suspend data transfers and impose draconian penalties on foreign companies; places onerous obligations on 'significant data fiduciaries'; and creates new and unreasonable criminal penalties and non-bailable offenses.

Other problematic measures and proposals on data localization in India have raised deep concerns for CompTIA members. The Reserve Bank of India issued a directive (RBI/2017-18/153), now in force, mandating aggressive localization requirements for data related to payment transactions. The directive requires "storage of data in a system in India" without clarifying whether the data can be accessed from or transferred outside the country, even if a copy is kept in India. Similarly, problematic data localization requirements exist in India's draft cloud computing policy and in a draft national e-commerce policy. We urge USTR to secure a strong commitment from Indian counterparts to avoid data localization measures in the Data Protection Bill, in the Reserve Bank of India Directive, and these other proposals.

Local Testing and Certification of Information Communications Technology (ICT) Products

India requires that manufacturers of ICT products register their products with laboratories affiliated or certified by the Bureau of Indian Standards (BIS), even if the products have already been certified by internationally accredited laboratories.[13] The Indian government has not articulated how such a domestic certification requirement advances India's legitimate public

[13] Electronics and Information Technology Goods (Requirement for Compulsory Registration) Order, 2012 (Oct. 3, 2012), https://www.crsbis.in/BIS/app_srv/tdc/gl/docs/gazette_notification_2012_10_03.pdf.

safety objective. U.S. stakeholders have raised concerns over delays in product registration due to the lack of government testing capacity, a cumbersome registration process, and tens of millions of dollars in additional compliance costs, which include factory-level and component–level testing. The domestic testing requirement is particularly burdensome for servers, storage, printing machines, and ICT products that are installed, operated, and maintained by professionals who are trained to manage the product's inherent safety risks.

Telecommunications, Communication and Information Services

In 2017, the Department of Telecommunications issued new draft requirements for in-country testing and certification of certain ICT equipment in the Procedure for Mandatory Testing & Certification of Telecommunications Equipment.[14] Like other testing regimes, these new requirements would mandate redundant and costly in-country testing for any company seeking to sell ICT products in India. These new requirements are separate from and in addition to the Compulsory Registration Order and the 2011 Telecom License Amendments.

If the Procedure for Certification of Telecommunications Equipment is implemented, U.S. ITC companies will face three distinct testing requirements that deviate from international norms and serve as significant market access barriers: (1) Compulsory Registration Order for safety testing; (2) telecommunications security testing under the 2011 Telecom License Amendments; and (3) the Department of Telecommunication's Procedure for Certification of Telecommunications Equipment.

Furthermore, India also differentiates between goods that are new, secondhand, remanufactured, reconditioned, and refurbished while assessing whether licenses should be required. CompTIA members continue to have challenges with this issue, particularly when obtaining licenses. Oftentimes, U.S. companies will run into challenges when there are procedural changes at Indian ports, particularly when there is a new customs officer. We urge USTR convey and secure a commitment from Indian counterparts to make the process of obtaining licenses smoother so as not to impede the importation of U.S. goods.

Indonesia

Cross-Border Data Flows

In October 2019, the Government of Indonesia issued updated legislation on data localization in Government Regulation No. 71 of 2019 (GR 71/2019). The new regulation shows some progress; however, CompTIA's members are still concerned over the scope of the provisions provided. Companies can store electronic data outside of Indonesia; however, doing so still remains subject to specific conditions: the location of the data storage outside Indonesia cannot negatively affect the supervision administered by a relevant state ministry or law enforcement agencies; and that access to the data storage and electronic data must be granted to the supervisors and law enforcement.

[14] Procedure for Mandatory Testing & Certification of Telecommunications Equipment (2017), http://tec.gov.in/pdf/Whatsnew/Final%20MTCTE%202017%20Procedure.pdf.

In addition, a GR 71/2019 includes provisions related to those found in previous legislation, the Minister of Communications and Informatics Regulation No. 20 of 2016; however, it incorporates a new set of principles and requirements for data protection. "Personal data" continues to be broadly defined to include any data about an individual who can be identified directly or indirectly by means of electronic or non-electronic systems. "Sensitive personal data" consists of data about a person's religion, beliefs, health, and financial status, among others. The law is likely to impact U.S. companies due to burdensome requirements that control the collection and cross-border transfer and use of personal data. Furthermore, GR 71/2019 is the first time Indonesia references "personal data controller" and fails to provide a concrete definition. The provision loosely alludes to what is found in the European Union's GDPR.[15] We urge USTR to address these barriers to U.S. firms' participation in Indonesian e-commerce, and to secure commitments from Indonesia to remove data localization measures and other unreasonably burdensome requirements.

Tariff Charges

On September 13, 2018, the Government of Indonesia's Ministry of Finance enacted a regulation that levied an additional 7.5 to 10 percent tax on certain imported goods, including technology sector products, ostensibly to protect its domestic industry in a manner inconsistent with its WTO commitments.[16] Further, the Ministry of Finance has shown interest in implementing classification provisions to the Harmonized Tariff Schedule by adding Chapter 99 to the Indonesia Customs Tariff Book entitled: "Software and other digital goods transmitted electronically." This was included in regulation PMK-17 enacted February 15, 2018 and came into force 14 days after the date of enactment.[17]

Telecommunications, Communication and Information Services

In August 2017, Indonesia's Ministry of Communication and Information Technology (MCIT) released a new draft regulation on OTT services. Some changes have been made to the draft since the 2016 version, but issues remain requiring OTT providers to set up a permanent establishment in Indonesia, offer terms of service in Indonesian language and use Indonesia's national payment gateway.

Japan

Cross-Border Data Flows

Japan's Act on the Protection of Personal Information (APPI) dating back to 2003, was amended with extensive reforms which impact the cross-border data transfer of personal and sensitive data.[18] The amendments took partial effect on January 1, 2016, and full effect on May 30, 2017. The amendments place additional restrictions on the collection and handling of

[15] Indonesia Issues Important New Regulation on Electronic (Network and Information) Systems. (October 2019). https://www.lexology.com/library/detail.aspx?g=cd6e5251-6dd7-4b46-b6be-759c78c9bf7b

[16] https://asia.nikkei.com/Economy/Indonesia-aims-to-raise-import-tariffs-on-900-consumer-items

[17] Determination of Goods Classification System and Charges of Import Duty Tariffs on Imported Goods, 17/PNK.010/2018 (Feb. 15, 2018), http://www.jdih.kemenkeu.go.id/fullText/2018/17~PMK.010~2018Per.pdf.

[18] Amended Act on the Protection of Personal Information, Ver. 2 (Dec. 2016), https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

personal data, including the requirement to obtain individual consent prior to the transfer of personal data to third parties outside of Japan. These laws will also apply extraterritorially to businesses outside of Japan who collect data from individuals located in Japan through the provision of goods or services. Japan has noted that it is committed to the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) system, and that certification of compliance to the CBPR system is a good way for companies to establish the requisite systemic protections to transfer personal information internationally.

Korea

Cross-Border Data Flows

In April 2016, Korea amended its Act on Promotion of Information and Communications Network Utilization and Information Protection, which imposes stringent protections on the personal data collected and handled by telecommunications and online service providers.[19] The amendments impose significant penalties for violating data protection standards, including punitive damages of up to three times actual damages for data breaches by service providers and forfeiture of profit gains obtained through violations of data privacy laws. In addition, telecommunications and online service providers must also obtain consent for any cross-border transfer. Failure to obtain consent results in a fine of up to 3 percent of the revenue related to the transfer.

Localization barriers regarding geospatial data continue to impede foreign internet services from offering online maps, navigational tools, and related applications in Korea. Separately, a new proposed bill would require online service providers whose daily average users exceed a certain threshold to establish local servers in order to ensure stability of user services. Penalties for not complying with this requirement would include up to a 3 percent fine based on revenue. This requirement appears to violate KORUS Art. 12.5 and Art. 15.8, which prohibit local server requirements and barriers to cross-border information flows.

Mexico

Digital Taxation

CompTIA members are highly concerned with Mexico's proposal in its 2020 Economic Budget Package that would impose discriminatory requirements on the digital economy and U.S. investment in Mexico's technology market. The proposal would require services that facilitate intermediate business transactions between users to withhold VAT (value-added tax) and income tax that would disproportionately affect U.S. industry. Mexico should continue to engage with the process at the OECD to develop a long-term solution for global taxation that does not disproportionately focus on a single sector of the global economy, or single out foreign companies for unique treatment.

[19] Act on Promotion of Information and Communications Network Utilization and Information Protection (promulgated March 22, 2016), http://www.law.go.kr/lsInfoP.do?lsiSeq=154247#0000.

Nigeria

Investment barriers

The National Information Technology Development Agency (NITDA) issued Guidelines for Nigerian Content Development in Information and Communications Technology in 2013.[20] The Guidelines requirements that multinational companies operating in Nigeria source all hardware products locally and that all government agencies source and procure all computer hardware only from NITDA-approved original equipment manufacturers. The Guidelines also require companies to use only locally manufactured SIM cards for telephone services and data and to use indigenous companies to build cell towers and base stations.

Philippines

Import Registration and Licensing Requirements

In 2018, the Philippine Optical Media Board (OMB) expanded the media subject to registration and licensing requirements, thus capturing Point of Sale hardware via Solid State Drives (SSD's) and most servers. The recent expansion of the media subject to these new requirements is overly burdensome on U.S. companies from an importation perspective, despite the purpose of these requirements to protect intellectual property rights.[21] We recommend that USTR petitions the Philippines government to roll-back the media expansion.

Saudi Arabia

Cross-Border Data Flows

Saudi Arabia's Communications and Information Technology Council (CITC) issued a Public Consultation Document on the Proposed Regulation for Cloud Computing, which contains a provision on data localization that may have the effect of restricting access to the Saudi market for foreign internet services. This regulation would also increase ISP liability, create burdensome new data protection and classification obligations, and require compliance with cybersecurity and law enforcement access provisions that are significantly out of step with global norms and security standards. Under this regulation, CITC would be granted broad powers to require Cloud and ICT service providers to install and maintain governmental filtering software on their networks. These and other ICT and Cloud regulations would also prohibit the cross-border transfer of certain classes of data.

Thailand

[20] Guidelines for Nigerian Content Development in Information and Communications Technology, https://nlipw.com/wp-content/uploads/Guidelines-for-Nigerian-Content-Development-in-Information-and-Communications-Technology-ICT.pdf.

[21] Republic of Philippines, Office of the President, Optical Media Board. Memorandum Circular No. 2018-002. (2018).

Telecommunications, Communication and Information Services

Thailand's National Broadcasting and Telecommunications Commission (the NBTC) finalized a governing policy on the classification of owners and operators of OTT services, which to date have been allowed to operate without a license. The intention of the policy is to subject owners and operators of onshore and offshore OTT services to the same or similar regulations as traditional broadcasters and telecommunications companies, including requirements to obtain and pay for operating licenses, pay a value added tax, and be subject to stringent checks on illegal content. We urge USTR to raise concerns with Thailand to regulate OTT services, which are often are delivered without a local presence and, should be treated with a flexible and light-touch framework.

Turkey

Cross-Border Data Flows

A Turkish E-Payment Law requires companies that provide electronic payment services to localize personal data servers in Turkey.[22] This law hinders U.S. companies from developing and expanding electronic services such as electronic invoicing, electronic general assembly and executive board meetings, electronic bookkeeping, new electronic payment and electronic money services.

Vietnam

Cross Border Data Flows

The Vietnamese Law on Cybersecurity (VLCS) was passed by the National Assembly on June 12, 2018. The law imposes burdensome requirements on companies in the name of cybersecurity, such as data localization, the policing of online content, ex-ante audits of hardware and software, and narrow timelines for incident notification, to name but a few.[23] The Ministry of Public Security (MOPS) recently introduced a new version of the draft Guiding Decree for the LOCS, subjecting almost all online services to severe data localization requirements in Vietnam as well as requirements to disclose data in unencrypted form to MOPS. While the MPS narrowed the localization requirement in August 2019, it is still too broad in nature and encompasses a vast majority of ICT products.[24] These requirements represent significant market access barriers in Vietnam for U.S. firms.

Other Trade Barriers Affecting CompTIA members

[22] Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions numbered 6493, dated 20 June 2013, published in the Official Gazette numbered 28690, dated 27 June 2013.

[23] See a description of the law on the Vietnam Business Law Blog, https://vietnam-business-law.info/blog/2018/7/30/vietnams-new-cybersecurity-law.

[24] Dang, T.S. & Seck, Y.C. (2019, October 18). *Vietnam: Updates to Draft Decree Detailing Certain Articles of Law on Cybersecurity.* Retrieved from https://globalcompliancenews.com/vietnam-updates-draft-decree-detailing-certain-articles-law-cybersecurity-20191008/

CompTIA members are also concerned with countries that have enacted measures harming market access through the regulation of "over-the-top" providers, holding ICT companies liable for third-party content, internet shutdowns, platform regulations, and unbalanced copyright laws:

Regulation of "Over-the-Top" Providers: Foreign governments display increasing interest in subjecting U.S. online services and applications to heavy-handed regulations designed for telecommunications or broadcast companies. These measures -- often called "Over-the-Top" or "OTT" regulations in foreign markets -- take different forms globally. However, it is increasingly common for regulators to seek to require online services to register as telecommunications providers, contribute to universal service funds, comply with technically infeasible emergency calling requirements, guarantee a particular quality of service, comply with local presence or data retention requirements, or take other steps that are not economically reasonable or technically feasible for non-telecom and non-broadcast services to implement. These regulations are resulting in market access barriers for U.S. services in **China, Colombia, European Union, India, Indonesia, the United Arab Emirates,** and **Vietnam**.

Holding ICT Companies Liable for Third-Party Content: CompTIA members are concerned at the rising trend of trading partners holding Internet intermediaries liable for third-party content and the related trend of unfeasible content-monitoring requirements. As highlighted by other commenters, there are inappropriate intermediary liability measures in place on copyright and/or non-copyright issues in **Germany**, **India**, **Indonesia**, **Russia**, **Thailand**, **Turkey**, **Ukraine**, and **Vietnam**. France appears to be creating a similar version of Germany's NetzDG law, which mandates removal of "manifestly unlawful" content within 24 hours and provides for penalties of up to 50 million Euros. At the EU level, there is now a proposal that would impose liability on companies that do not meet unreasonable requirements to remove content within one hour of notification, including a financial penalty of up to 4 percent of global turnover in case of 'systemic failures' to remove certain types of harmful content. In addition, countries including **Australia**, **Colombia**, and **Peru** have failed to implement their obligations under trade agreements with the U.S. to establish safe harbors from liability reflecting Section 512 of the Digital Millennium Copyright Act.

Internet Shutdowns: CompTIA also notes with concern that many countries including **Algeria, Bangladesh, Brazil, Egypt, Ethiopia, India, Iraq, Morocco, Pakistan, the Republic of the Congo, Saudi Arabia, Syria, Turkey** and **Vietnam** have continued the alarming trend of shutting down domestic Internet or mobile services. In addition to limiting freedom of expression, these policies impact U.S. companies that are unable to engage in business activity within these countries during periods of Internet disruption.[25] Additionally, in **Algeria, Iraq**, and **Uzbekistan**, telecommunications companies have been ordered to shut down the internet during academic testing season to prevent cheating.

Other Platform Regulation: New proposed regulations on "platform-to-business" (P2B) relations in the **EU** would require online intermediaries to provide redress mechanisms and meet aggressive transparency obligations concerning delisting, ranking, differentiated treatment, and

[25] For more information regarding Internet shutdowns, please see Accessnow.org, https://www.accessnow.org/keepiton/.

access to data. These rules would apply not just to marketplaces with business users but also to non-contractual relations between businesses and platforms, and would ban various forms of "vertical integration" while potentially requiring the disclosure of "criteria, processes, specific signals incorporated into algorithms or other adjustment or demotion mechanisms used in connection with the ranking." CompTIA encourages USTR to monitor these developments closely.

Unbalanced Copyright Laws: CompTIA members are also concerned that countries have enacted copyright laws that fail to account for important exceptions and limitations, such as fair use. Those policies create trade barriers for U.S. internet service providers who rely on balanced copyright laws and protections to innovate and conduct business across borders. For example, **France, Germany**, and **Spain** have all implemented some version of 'ancillary copyright' measures that place undue restrictions on the use of text or images by U.S. companies. In addition, CompTIA members are concerned that the EU has proposed new copyright rules that would serve as a barrier to US services. USTR has previously found that ancillary copyright rules are "key barriers to digital trade," yet the recent proposed text from the European Parliament would prohibit online services from linking or pointing to articles without payment, imposing particular restrictions on publishers' freedom to choose their business model. Similar rules could also extend to images under Article 13b of the European Parliament text. Finally, Article 13 of the European Parliament text includes new direct liability measures for content uploaded by users and would consequently amount to mandatory content filtering requirements for a wide variety of U.S. services, including cloud and enterprise services. This proposal bears no resemblance to U.S. law and the recently negotiated position under the U.S.-Mexico-Canada Agreement, and fails to include much-needed safeguards. We urge USTR to engage quickly with European counterparts to ensure a consistent transatlantic approach to copyright law and to remove measures that will create digital market access barriers.