BSA Written Statement
Investigation No. 332-561
Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions

April 21, 2017

Ms. Lisa R. Barton
Secretary
United States International Trade Commission
500 E Street SW
Washington, DC 20436

Re: Written Statement – Investigation # 332-561

BSA | The Software Alliance[1] welcomes the opportunity to provide information concerning significant barriers to digital trade to help inform the investigation being conducted by the United States International Trade Commission (USITC).

Software innovation is transforming every sector of the American economy and enriching every aspect of our lives. Software has a profound impact on the American economy. A recent BSA study shows the software industry contributes more than $1 trillion to the US GDP, nearly 10 million jobs, and $52 billion in research and development (with significant impact in each of the 50 states), which expands America's economic potential across numerous sectors. This economic progress, coupled with tens of billions of dollars in software research and development investments, translates into software serving as a powerful catalyst for economic change – making businesses more effective and the US economy more prosperous.

The ability of US companies to continue to lead global advances in innovative technology is under a rising threat from governmental measures hampering their business models, and especially the crucial role played by international movement of data. The way in which software is used and delivered is changing rapidly. Whereas BSA members once delivered their software to consumers primarily on CD-ROMs or pre-installed on PCs, today software is more often downloaded online or used on remote servers, such as through cloud computing services.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro, and Workday.

The trade barriers the software industry faces are also changing. Polices that impact companies' ability to move data across borders, that require the disclosure of proprietary information, and that mandate the use of local content and/or technology are some of the examples of the barriers companies face today.

Barriers to cross-border data flows are often disguised as privacy or security measures. Cross-border data flows are key to the current and future success of not only the software industry but also of all other sectors of the US economy. The importance of cross-border data flows will increase in coming years, and, thus, immediate attention to these threats is urgently needed.

Our comments will focus on the aspect of your investigation that will seek to identify regulatory and policy measures that may significantly imped or hamper digital trade. We will highlight existing or proposed policies that create significant barriers in areas including:

Cross-Border Data Flows: The trade disruptive impact of measures that impede the movement of data across borders is immense and affect all sectors of the economy. Data-related market access barriers take many forms. Sometimes countries expressly require data to stay in-country or impose unreasonable conditions to send it abroad; in other cases, they require the use of domestic data centers or other equipment. These barriers are often disguised as **privacy** or **security** measures. Unfortunately, a number of markets, including Brazil, China, India, Indonesia, have adopted or proposed rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory. We are also closely following developments in the EU that could pose significant barriers to providing digital services in the market.

Disclosure of Proprietary Information: Policies that require the disclosure of source code or other proprietary information as a condition for market access represent enormous market access barriers for BSA members. Countries with existing or proposing such policies include Brazil, China, Indonesia.

Local Content and Indigenous Technology: Policies that require information technology products to include a certain percentage of local content and/or mandate the use of locally developed technology as a condition for market access are barriers to digital trade. Countries with or proposing such policies include China, and Indonesia.

Government Procurement: Several countries are imposing or considering significant restrictions on foreign suppliers' ability to serve public-sector customers. Countries with existing or proposed restrictions against public procurement for foreign software products and services include Brazil, China, and, India.

Standards and Local Testing: Country-specific standards and local testing requirements create *de facto* trade barriers, raising the costs of cutting-edge technologies for consumers and enterprises. Countries with existing or proposing such policies include Brazil, China, India, Indonesia.

Technology Neutral Patent Protection: Intellectual property protection is a key driver of R&D investments by enabling US companies to commercialize their innovations. It is paramount that countries provide effective patent protection to eligible computer-implemented inventions, in line with their international obligations. Negative developments in this area hurt innovative companies and need to be addressed. For example, India's current approach to patentability of computer-related inventions is out of step with international practices and will prevent most computer-related inventions from being eligible for patent protection.

Balanced Copyright Protection and Safe Harbors: Like other desirable digital content, software is subject to extraordinarily high volumes of infringement. A recent IDC study estimated the commercial value of unlicensed software use to be more than $60 billion.[2] We therefore support policies that ensure

[2] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

that legal remedies are available for right holders to address copyright, including in the online environment. To ensure such policies will not stifle the Internet's potential as a medium for free expression, innovation and digital commerce, it is critically important to provide online service providers with appropriate safe harbors from liability for infringing (or otherwise unlawful) content posted by third parties. Such safe harbors should not be conditioned on any obligation by the ISP to monitor or filter infringing activity as such obligations would weaken incentives for innovation and threaten the dynamism and values that have made the Internet so valuable.

In the following sections of this submission, BSA provides country-specific information on countries your investigation focuses on and that have implemented or are considering policies that represent significant market access and barriers to US products and services. Our comments relate to China, India, Indonesia, the EU, and Brazil.

We commend the USITC for conducting this important investigation and we look forward to contributing to your efforts. We stand ready to answer any questions you may have.

ASIA

CHINA

Overview:

The commercial environment in China for software and information technology is very challenging. The Government of China continues to issue security-related policies that effectively act as procurement preferences and other market access barriers. These include sweeping security-related legislation, as well as sector-specific cybersecurity regulations for the banking and insurance sectors, which request or require firms in these sectors to replace existing systems with "secure and controllable" products and services. BSA members are very concerned that these policies could effectively block them and other US suppliers from an increasing number of important sectors in the Chinese economy.

China's existing regulatory regime also makes it extremely difficult for BSA members to invest in the digital market. There has been very limited progress in reforming the existing system, which effectively excludes foreign investment especially in cloud or other data services in China. Except for a conditional and limited opening in the electronic commerce field, China continues to regulate Internet services as value-added telecommunications services (VATS) and precludes granting licenses to wholly-owned or majority-owned foreign entities.

These policies, combined with broader "indigenous innovation" policies, contribute to an increasingly challenging market access environment for many BSA members. These policies negatively affect market access by US companies.

The intellectual property (IP) environment is also extremely challenging in China and negatively impacts market access. BSA is monitoring developments related to policy and legal developments regarding competition policy and the utilization of patents and other IP, as well as patent law reform.

Specific Concerns*:*

Counter-Terrorism Law*:* In December 2015, China passed the Counter-Terrorism Law. BSA, like other associations, provided comments, including raising concerns that some provisions impose vague and/or burdensome requirements on companies that may not be the most efficient way to curb terrorism. For example, telecommunication business operators and Internet service providers are generally obliged to "provide technical support and assistance, such as technical access and decryption" to law enforcement agencies, and appear to be required to monitor content for extremist communication. It remains unclear whether these measures will require companies to use weaker forms of encryption in their products than are currently available, thereby making their products more vulnerable to cyber theft.

Cybersecurity Law: In November 2016, the National Peoples' Congress passed the Cybersecurity Law that would create a firmer legal basis for the activities of the Cybersecurity Administration of China, impose a variety of obligations on "network providers", impose additional security and testing requirements and national security "reviews" on the procurement of certain software and IT products and services for "Critical Information Infrastructure" operators, limit data flows, and establish a prescriptive personal data protection regime. A number of regulations implementing the law are being considered and, if implemented as draft, would further exacerbate these concerns. The Government of China should adopt rules implementing the Cybersecurity Law enhancing the cybersecurity capabilities of enterprises and other institutions in a manner consistent with international standards and approaches, that do not impose unnecessary administrative compliance burdens, and do not discriminate against BSA members and other foreign companies.

Regulation on Cloud Services: In November 2016, the Ministry of Industry and Information Technology (MIIT) published a Draft Notice on Regulating Business Operation in Cloud Services Market (Draft Notice). BSA and other associations submitted comments to the Government of China raising concerns

about the Draft Notice and its implications for the operation of foreign cloud business in the country. These concerns include important IP-related issues, requirements to utilize infrastructure and maintain data in China limiting data flows, among other issues.

"Secure and Controllable" Policies: In addition to legislative developments, there have been several security-related regulatory developments that raise significant market access concerns. Sectoral regulators, such as the China Banking Regulatory Commission and the China Insurance Regulatory Commission continue to develop "secure and controllable" policies that require regulated private firms and state-owned entities (SOEs) to procure only designated "secure and controllable" products, software, and services. "Secure and controllable" has been widely interpreted by affected entities as referring to "domestic" as opposed to foreign IT products, software and services.

Indigenous Technology Requirements: BSA continues to urge reform of long-standing measures, such as the Multi-Level Protection Scheme (MLPS). The MLPS imposes significant restrictions on procurement of software and other information security products for an overly broad range of information systems the government considers sensitive. Among other requirements, procurements of such products are limited to those with intellectual property rights (IPR) owned in China. This applies to procurements by the Government of China and increasingly to procurements by SOEs and private sector entities, restricting market access restriction for foreign information security products. As a result, many entities in China are unable to procure the most effective security tools to meet their needs.

Encryption: China maintains its 1999 Commercial Encryption Regulations, which state that 1) entities importing, developing, and selling encryption technology in China must obtain a license from the State Encryption Management Bureau (SEMB), including a special license to apply to use foreign encryption technology; 2) encryption products sold in China must be subject to testing that requires disclosure of source code in order to receive a sales license; and 3) foreign technology providers must use Chinese indigenously developed encryption technology, particularly algorithms. These regulations remain a significant barrier to foreign security products, particularly if authorities begin applying the regulations more broadly. The regulations also run counter to China's agreement with five other countries in 2013 to adopt the World Semiconductor Council Encryption Best Practices. These Best Practices, among other things, prohibit the regulation of encryption used in commercial ICT products that are imported or sold domestically. These concerns would be further aggravated if the Cryptography Law released in draft format for public comments in April 2017 is not modified.

VATS Licensing: China's authorities, principally the Ministry of Industry and Information Technology (MIIT), require companies wishing to provide Internet-based services or content to acquire VATS licenses. For example, companies wishing to provide web- or cloud-based content services must acquire an Internet content provider (ICP) license. However, foreign invested enterprises are not allowed to acquire such a license. By regulation, foreign firms wishing to acquire such a license must establish a foreign invested telecommunication entity (FITE), which must contain less than 50 percent foreign equity. Worse, in practice, MIIT has not issued new ICP licenses to FITEs. Similarly, foreign firms are restricted from running data centers in China because they have no opportunity to acquire the necessary Internet data center (IDC) license.

Intellectual Property and Competition: The State Council's Anti-Monopoly Commission (AMC) recently issued draft rules regarding the abuse, or misuse, of intellectual property rights (IPR) under the Anti-Monopoly Law (AML). BSA members remain concerned that discretion granted to local Anti-Monopoly Law (AML) enforcement agencies may expose rights holders to administrative abuse or allow AML-enforcement agencies to use AML enforcement for industrial policy or other protectionist purposes. Specific concerns include applying rules tailored to standard essential patents to non-essential patents not encumbered with voluntary fair, reasonable and non-discriminatory (FRAND) licensing commitments. The US Government should continue to urge China to avoid using AML enforcement to undermine or prevent the normal and legitimate exercise of IPR.

Patent Enforcement: The State Intellectual Property Office (SIPO) has proposed amendments to the Patent Law. Among other things, the proposed amendments would expand the enforcement powers of SIPO and its subsidiary agencies at the provincial and local levels of government. These agencies would then be able to conduct *ex officio* raids and enforcement actions against ill-defined "market-disruptive" patent infringement activities, and award fines and other penalties. This creates enormous risks for patent holders in China. The Chinese judicial system is the proper forum to adjudicate patent infringement and damages, and it is improper to vest that same authority in administrative agencies as well. The proposed empowerment of SIPO and hundreds of local intellectual property offices (IPOs) in enforcing patents will dramatically change the current enforcement landscape, creating the potential for substantial confusion and duplication of the role that courts now play. The envisioned role for SIPO and IPOs as patent enforcement authorities is, based on our research, without analogue in any other national law.

INDIA

Overview:

The Government of India (GOI), at the central and state levels, has adopted a variety of policies affecting market access to BSA members and the IT sector more generally. Policies are sometimes not developed with adequate consultation with stakeholders and are implemented in confusing and inconsistent manners. This has created a substantial and negative impact on IT sector investment and growth in India. Additional concerns include domestic preferences and technology mandates in public procurement, as well as a confusing regulatory environment regarding security and privacy.

Specific Concerns:

Cross-Border Data Flows: Data and server localization requirements are imposed in a heterogeneous manner across regulatory structures and procurement contracts in India. For example, in 2015 the Department of Electronics and Information Technology (DeitY), which is now the Ministry of Electronics and Information Technology (MeitY), issued guidelines for a cloud computing empanelment process by which cloud computing service providers (CSPs) may be provisionally accredited as eligible CSPs for government procurements of cloud services. However, the policy requires that CSPs must store all data in India to qualify for the accreditation. There is strong evidence that such policies are harmful to India as they reduce productivity and dampen domestic investment in the country.[3]

Similarly, the draft Machine-to-Machine (M2M) Roadmap, issued by the Department of Telecommunication (DOT) in January 2015, proposed to require all M2M gateways and servers be located in India "in the interest of national security." BSA was grateful that the DOT removed this unnecessary and counter-productive requirement in the final M2M Roadmap issued May 12, 2015.[4] However, India is currently working on implementation of the roadmap and data localization mandates are once again being considered.

Another example is the 2012 National Data Sharing and Accessibility Policy, issued by the Ministry of Science & Technology, which imposes onerous data localization requirements for weather data. This localization requirement will undermine the ability of global ICT companies to offer cutting-edge smarter cities and disaster management solutions as part of Digital India.

Encryption: Most other countries allow the use of strong encryption standards ranging from 128-bit to 256-bit to ensure the security of sensitive information exchanged via the Internet and other networks. In India, however, only 40-bit encryption can be used without additional regulatory approval, according to the DOT's Guidelines for the Grant of License for Operating Internet Service (ISP Guidelines). Encryption standards differ greatly from one regulatory agency to another, since each one has its own specific set. In September 2015, DeitY published a draft National Encryption Policy, and then quickly withdrew the draft. The draft policy raised a number of concerns including restrictions on the use of commercially available encryption (by restricting key lengths, for example) and mandates to disclose proprietary information. India is currently working on a new draft encryption policy that could potentially introduce market access barriers if issues are not properly addressed.

Cloud Computing: In June 2016, the Telecommunications Regulatory Authority of India (TRAI) released a draft Cloud Computing Consultation Paper. The consultation paper requested stakeholder input on a range of important questions regarding cloud computing, and BSA was grateful for the opportunity to review the questions and present responses on behalf of our members. Many of the questions' topics, such as interoperability, platform-to-platform migration, and others are currently best addressed by CSP-to-customer arrangements (such as contracts) and would not benefit from broad government intervention. We would be particularly concerned if TRAI or other GOI agencies determined that requirements to localize data or impose India-unique standards or approaches were necessary to address the questions

[3] http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.
[4] http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

raised in the consultation paper. Cloud computing remains in a relatively early stage of development, and for many of the issues raised in the consultation paper an overly-regulated approach is likely to inhibit development, deployment, and growth of cloud computing services, which would be detrimental to US companies wishing to serve the Indian market.

Patentability Guidelines for Computer Related Inventions: The Office of the Controller General of Patents, Designs, and Trade Marks (CGPDT) issued Revised Guidelines for Examination of Computer Related Inventions (CRIs) ('Guidelines') on August 21, 2015. The Guidelines – the product of several years of deliberation, stakeholder engagement, and study – were an improvement over earlier versions and appeared to settle uncertainty over whether software-enabled inventions were eligible for patent protection in India. Unfortunately, in late 2015 the Guidelines were suspended after the GOI received concerns from groups representing civil society and other stakeholders. In February 2016, without any formal public consultations, the CGPDT issued significantly revised guidelines. The new guidelines prevent most software-enabled inventions from receiving patent protection in India. The guidelines appear to require a computer-related invention to include novel hardware in order to be eligible for patent protection. This is out of step with international practice and potentially in conflict with India's obligations under the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). Patent protection is vital to the software industry and it is important that the Guidelines provide clarity to patent examiners on how to properly apply the Patent Act to applications for CRIs. As the GOI continues to consider further revisions to the examination guidelines, BSA urges the US Government to continue engaging the GOI to ensure that patent protection is available for CRIs consistent with global practices.

Procurement: DeitY has mandated the use of open source software in e-governance. The policy's objective is to reduce the price of IT projects. However, this mandate is unlikely to help the government achieve this objective, and may undermine the Digital India program goals more broadly. In fact, this mandate, as written, could significantly limit the choices available to government agencies, decrease competition and innovation, and fail to deliver savings by failing to take into account the total cost of the implementation and operation of IT projects. In addition, specific requirements or policies that mandate the use of certain technologies undermine security by restricting the use of evolving security controls and best practices, and potentially creating single points of failure. India would benefit by formalizing its existing procurement practices and clearly eliminating laws and policies that 1) condition access to government procurement on the use of particular technologies or licensing models (for example, mandates for use of open source software over proprietary software); or 2) condition access to government procurement on a product or service having intellectual property that has been locally developed or registered.

INDONESIA

Overview:

A variety of policies affecting the IT industry have been developed or proposed over the last several years that make or threaten to make it increasingly difficult to provide digital products and services to the Indonesian market. This creates a very challenging commercial environment for the software and (IT sector in Indonesia.

Specific Concerns:

Data Localization Requirements and Cross-Border Data Flows: The Indonesian Ministry of Communication and Information Technology (MCIT) enacted the Regulation on the Protection of Personal Data in Electronic Systems in December 2016. The regulation raises concerns regarding data localization mandates, unreasonable obligations on data service providers, and other matters. Such requirements will increase costs, harm the quality of data services, and interfere with the assurance of data security without the enhancement of personal information protection.

In addition, in October 2015, the Government of Indonesia initiated a draft bill on the Protection of Private Data (also referred to as the Draft Privacy Law), which is currently being discussed by the House of Representatives. Should it pass, the bill would represent Indonesia's first overarching law on data privacy. Thus far, however, the government has not consulted the public on the Draft Privacy Law. It is also presently unclear how it would interact with the Draft Electronic Data Protection Regulation. This creates legal uncertainty that negatively impacts US companies access to the Indonesian market.

Local Content and Local Manufacturing Requirements: In 2015, MCIT issued the Ministerial Decree on Local Content for LTE Technology, which imposes onerous local content requirements on a wide range of technology devices and products. The decree was signed jointly by MCIT and the Ministries of Trade and Industry in early July 2015, and is expected to be strictly enforced by January 2017. The rules require that all covered products would need to contain 30-40 percent local content (depending on the particular product) in order to be sold in Indonesia. The Ministry of Industry confirmed in July 2015 that local content includes both hardware and software[5].

Closely related to the issue of local content, the Ministry of Trade passed regulations in 2013 requiring importers of certain IT products (including smartphones, laptops, and tablets) to establish local manufacturing facilities within three years from the date of obtaining their import license. If strictly enforced, this will effectively prevent the import of foreign-made IT products into Indonesia.

The stated purpose of these policies is to encourage local manufacturing and industry development. We believe that Indonesia can better achieve its economic objectives through regulatory policies that incentivize the development of knowledge-based industries, such as software and application development, rather than through the adoption of market access barriers such as local content and local manufacturing requirements.

Accreditation of Auditors and Certification of Security Requirements: The Government of Indonesia released a Draft Information Security System Regulation in July 2015. The draft regulation requires strategic and high-electronic system providers to undergo a risk assessment to obtain certification against the ISO/IEC 27001 standard. However, testing against the standard must be performed locally by an in-house Indonesian expert or by an expatriate. BSA urges the US Government to work with the Indonesian Government to stress the importance of recognizing the validity of certifications obtained from

[5] The Ministry of Industry is still formulating the methodology for calculating the local content percentage. While the methodology will allow for software (e.g. apps) to count toward (and even comprise the entire) local content percentage, this will only be for software that is locally produced and run out of local data centers. It will not be possible, for example, to take into account the overall economic contributions that foreign software corporations make to the Indonesian economy (e.g. software donations or other investments).

internationally accredited testing organizations. Requiring duplicative in-country testing will ultimately drive up the cost of computer and information systems, creating market access barriers without advancing any corresponding security benefits.

Source Code Disclosure Requirement: The Indonesian government released a draft Regulation on Electronic Systems Software in July 2015. If implemented as drafted, the regulation would require electronic system providers responsible for managing or operating computer systems used in connection with public services to disclose software source code. BSA is deeply concerned with this requirement. Many global companies providing leading-edge security technologies would need to withdraw from bidding opportunities that would require them to turn over or make available their intellectual property, such as source code and other design information. As of September 2016, the regulation was still pending.

OTT Regulation: In early 2016, the MCIT issued draft regulations regarding the Provision of Application and/or Content Services Through the Internet, referred to as "OTT Rules." These rules threaten to impose unreasonable requirements on virtually all Internet-enabled services and service providers, including local permanent establishment mandates, use of local payment gateways, and unclear data retention policies among others. As of April 2017, the regulation was still pending.

EUROPEAN UNION

Overview:

The market access environment in Europe for BSA members has become increasingly challenging. European authorities, both at the member state level and at the level of the European Union, are increasingly considering or adopting market access barriers often justified on security or privacy grounds. These barriers affect the ability of BSA members to compete effectively in the market and provide the cutting-edge technologies and services increasingly demanded by costumers in the EU. BSA members are very concerned because this trend is likely to become more intense in the coming years.

EUROPEAN UNION

Data Flows: Measures that impede the flow of data across borders impose substantial burdens on US providers of such services and negatively impact US jobs. European authorities are focused on data transfers by US companies to the United States, and have not applied the same scrutiny to data transfers to any other market — large or small — including key markets such as China, Japan, South Korea, and Russia.

The US-EU Privacy Shield, which replaced the former Safe Harbor framework for data transfer from Europe to the United States, took effect on August 1, 2016, and represents a strong agreement to foster transatlantic data transfers while safeguarding consumer privacy. It was immediately challenged before the European Court of Justice (ECJ) in cases brought by two privacy activist groups (Digital Rights Ireland and La Quadrature du Net). Further challenges before the national courts of EU member states are expected. These groups contend that the Privacy Shield should be invalidated for the same fundamental rights reasons that were the basis for the ECJ's 2015 invalidation of the previous Safe Harbor framework, specifically they contend that US practices on law enforcement and national security access to data lack sufficient privacy safeguards. These legal challenges, along with the upcoming first annual review of the Privacy Shield in September 2017, mean US companies will face continuing uncertainty in relying on the Privacy Shield for transatlantic data transfers.

Standard contractual clauses, a second major mechanism used to transfer data from Europe to the United States and other countries, is under judicial review in Ireland and the case is likely to be referred to the ECJ in 2017. The Irish Data Protection Commissioner contends that standard clauses also are not consistent with EU fundamental rights law when they are used as a basis for data transfers to the United States. Thus, companies relying upon standard clauses for this purpose are also at substantial risk in their European operations.

Both sets of legal challenges are predicated on the assumption that US surveillance laws do not effectively protect the personal data of EU citizens. However, no other country's surveillance practices have been scrutinized regarding their implications for the validity of data transfers from Europe nor has the EU scrutinized or applied the same standards on the surveillance practices of its own member states.

Proliferating data localization laws in EU member states pose a barrier. For example, a November 2016 French government report calls for data localization and justified its position in part with clear anti-American economic motivation. According to the report[6]: "French and European hosting companies see data location as an opportunity to stand out from the existing, primarily US, service offering." And further, "Moreover, the USA has a substantial competitive advantage in this sector, that the enshrinement of the free data flow principle would automatically strengthen."

The US Government had sought to limit data localization measures in the now-suspended Transatlantic Trade and Investment Partnership (TTIP) and Trade in Services Agreement (TISA) negotiations. The EU

[6] "The Free Flow of Data in International Commercial Agreements". Executive Summary in English available at http://www.economie.gouv.fr/files/files/PDF/Executive_summary_digital_in_trade_agreements.pdf

refused to discuss the subject in either negotiation. In addition, the European Commission announced in late 2016 that it was abandoning plans to propose legislation restricting member states' abilities to enact data localization members.

Proposed e-Privacy Regulation: In January 2017, the European Commission proposed a sweeping revision of its existing e-Privacy Directive that would transform it into a regulation. The scope of the proposed regulation would expand substantially, from telecommunications services to any electronic communications services provided with the use of a public communications network, including over-the-top services and the conveyance of machine-to-machine communications for use in the Internet of Things. It also would apply extraterritorially, where processing is conducted outside the EU in connection with services provided within the EU.

Among the onerous requirements that would be imposed on data-related businesses are: confidentiality requirements that would restrict commercial uses of metadata (such as traffic data) and content data without user consent; stricter, express consent requirements, including for the use of cookies for profiling and data analysis; creating a foreseeable conflict of law regarding the obligations to respond to data requests from EU governments. Violations of the proposed regulation's provisions would carry heavy administrative penalties at the level of the General Data Protection Regulation (see below).

General Data Protection Regulation (GDPR) Implementation: The GDPR was adopted in April 2016 and will apply across the EU in May 2018. EU member state data protection authorities and the Commission have begun to issue implementing measures. It is critical for both the US and EU economies that the GDPR strike the right balance between protecting privacy and fostering the transatlantic digital economy. However, the data protection authorities have declined to establish a formal mechanism for consulting stakeholders on implementing measures. Clear implementing measures grounded in practical experience are extremely important, as companies need to be able to comply with them or risk heavy fines that could reach up to 4 percent of annual global corporate turn-over.

Copyright – Text Data and Mining: Text and data mining (TDM) involves the automated computational analysis of information in digital form to uncover patterns and underlying facts from large datasets. US companies are leaders in data analytics research and development, including in the EU.

Under current EU law, TDM performed on lawfully accessed works neither conflicts with the normal exploitation of such works nor undermines the legitimate interests of authors. In 2016, however, the European Commission proposed a digital copyright directive that would create uncertainty about the legality of TDM under the existing copyright framework. The Commission proposal would affirmatively allow only public interest research organizations engaged in scientific research to conduct TDM, thereby creating an implication that such activity, when performed by commercial entities, falls outside of the existing temporary copy exception. Any entity that has lawful access to data should be permitted to perform TDM and analytics on that data, regardless of the entity's status as a research organization or commercial entity. Uncertainty about whether this rule would continue to prevail in the EU operates as a market access barrier to US data analytics companies.

Digital Content Directive: The proposed Digital Content Directive would introduce potentially burdensome rules with respect to the supply of digital content to consumers, including software and cloud services. It might also impact business-to-business transactions. For example, the directive would impose an onerous and ill-defined requirement to return consumers' data (personal data and non-personal data) at the conclusion of a contract. Because the scope of this obligation is inadequately defined, it could require companies to return enormous volumes of proprietary data created by a company during the course of providing online services (e.g., quality assurance data, telemetric data, and cybersecurity data). Ongoing legislative consideration of the Digital Content Directive could also result in reclassification of software embedded in consumer devices as "goods," thereby exposing companies to increased liability for consequential damages.

LATIN AMERICA

BRAZIL

Overview:

President Temer's new Administration has demonstrated willingness to engage in a more open dialogue with stakeholders, which could result in an improvement in the current policy framework, but the overall market environment in Brazil remains challenging. A variety of existing and proposed measures related to privacy and public procurement preferences have created, or could bring about, de facto market access barriers to BSA members' products and services. We urge the US Government to continue engaging the Brazilian Government in a dialogue targeted at eliminating the trade barriers these measures represent.

Specific Concerns:

Data Flows: Brazil's long-debated personal data protection regulation reflects the perceived need for legislation governing the personal data of Brazilian citizens. Since industry and civil society successfully urged Congress to drop onerous provisions for data center localization from the final text of the Marco Civil da Internet Law (Marco Civil), focus has shifted to the Personal Data Protection Bill to address outstanding aspects of personal data and privacy protection.

Although there have been improvements vis-à-vis initial drafts of the privacy bills that are currently being considered by the Brazilian Congress, the most recent drafts still raise concerns. Concerns based on current drafts include extra-territorial application of the Brazilian law, potential for explicit consent being required to legitimate a wide range of data treatment operations, restrictions on cross-border data flows, unreasonable liability on data processors, and other issues concerning the implementation of the law that could create legal uncertainties. These issues need to be addressed to avoid adverse impact on US companies operating in the Brazilian market.

In addition, in March 2017, the Government of Brazil issued Draft Guidelines for Public Procurement of Cloud Computing Services, which contains a number of concerning provisions including server and data localization requirements.

Government Procurement Barriers: Presidential Decree 8135/2013 (Decree 8135) regulates the use of IT services provided to the Federal government by privately and state-owned companies, including the provision that Federal IT communications be hosted by Federal IT agencies. In 2015, the Ministry of Planning developed regulations to implement Decree 8135, which include: technical specifications for standardized services; contract rules, conditions, and prices; interoperability standards; management of agency solicitation of services; and periodic price review. The regulations present multiple serious problems for BSA members, especially the deviation from global standards and requirements to disclose source code and other intellectual property. On August 9, 2016, the new Secretary of Information Technology for the Ministry of Planning announced that the Federal government will revoke Decree 8135/2013. A new decree was expected to be published in 2016, but is still pending.

Government Procurement Preferences: CERTICs (Certification of National Technology Software and Related Services) is the certification component of the *TI Maior* Industrial Plan, conferring public procurement preferences to software developed in Brazil. CERTICs has not been recently applied, but the policy has not been rescinded. Annex I of Decree 8186/14 (January 17, 2014) establishes an 18 percent price preference for the following categories: software licenses; software application development services (customized and un-customized); and maintenance contracts for apps and programs.
In addition, the Brazilian Congress is currently discussing potential changes to Brazil's Procurement Law. The current law allows the public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of IT systems to be limited to local goods and services only when such products and/or services are classified as "strategic" by a decree published by the government. A bill currently pending Congressional approval could remove the need for a decree

classifying products and services as strategic. Should the bill be approved, any public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of IT systems could be limited exclusively to local goods and services, creating a market access barrier for foreign companies.

***Open Source Preference*:** Proposed legislation (PL 2269/1999) would require the use of open source software by government entities and state-owned enterprises (SOEs). The legislation had been stalled for some time, but it was resubmitted at the beginning of the 2016 session with new favorable reports and a sponsor interested in forwarding the issue, although this has not happened so far. BSA has consistently argued that procurement decisions should be based on choosing the best products and services available to meet the specific requirements, without preferences or mandates based on particular technologies or licensing models, taking into account the entire life-cycle cost of a product or service and not just the upfront fees or royalties.