BSA Comments on Foreign Trade Barriers to US Exports for 2017 National Trade Estimate Reporting

October 27, 2016

Docket No. USTR-2016-0007
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

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. 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 the US economy, and their importance will only increase in coming years. Immediate attention to these threats is urgently needed.

BSA | The Software Alliance[1] provides the following submission concerning significant barriers to US export of goods and services, US foreign direct investment, and protection of intellectual property, to be considered for inclusion in the annual National Trade Estimate Report on Foreign Trade Barriers (NTE).

In response to your specific request, several of our comments relate to localization barriers to data services and digital trade. Such barriers are increasing and are of major concern to our members. We commend your special focus on this subject. Our comments are also intended to reinforce information BSA previously submitted to USTR pursuant to the Special 301 statutory mandate, identifying countries that deny fair and equitable market access to US companies that rely upon intellectual property protection.

Significant trade barriers include:

Cross-border data flows: Data-related market access barrier requirements 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.

Recognizing the trade disruptive impact of measures that impede cross-border data flows, the United States succeeded in including specific enforceable obligations relating to such practices in the recently

[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, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

concluded Trans-Pacific Partnership Agreement (TPP).[2] BSA strongly supports this important outcome and urges the US Government to seek similar enforceable obligations through all available trade mechanisms, including other trade negotiations, the Special 301 and NTE processes.

Privacy: Governments increasingly use privacy policies to rationalize imposing limits on international data flows, which operate as disguised restrictions on trade.

Security: Governments around the world are also using or proposing to use security concerns to justify the creation of trade barriers.

Government Procurement: Several countries are imposing significant restrictions on foreign suppliers' ability to serve public-sector customers.

Standards: Some countries have developed or are developing country-specific standards for software and related services. This creates a de facto trade barrier, raising the costs of cutting-edge technologies for consumers and enterprises.

BSA is the leading advocate for the global software industry in the United States and abroad. Our members are at the forefront of driving the global digital economy, and invest substantial resources into developing cutting-edge technologies. These companies strongly rely on intellectual property protection and access to foreign markets to continue innovating.

In the following sections of this submission, BSA provides country-specific information on US trading partners that have implemented or are considering policies that represent significant market access and barriers to US exports of goods and services, and US foreign direct investment. Our comments relate to China, India, Indonesia, Japan, Republic of Korea, Thailand, Vietnam, the European Union, Germany, the United Kingdom, and Brazil.

We stand ready to answer any questions you may have.

[2] TPP Agreement – Articles 14.11 and 14.13 available at https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text

TABLE OF CONTENTS

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. Although the final law does not include detrimental requirements that were present in an earlier draft, BSA remains concerned with provisions that impose vague and/or burdensome requirements on software and IT companies that will not effectively curb terrorism and will create trade barriers. For example, the law appears to require telecommunication business operators and Internet service providers to monitor content for extremist communication.

Cybersecurity and "Secure and Controllable" Policies: Sectoral regulators, such as the China Banking Regulatory Commission (CBRC) and the China Insurance Regulatory Commission (CIRC) continue to develop "secure and controllable" policies that require regulated private firms and state-owned entities 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.

***Cybersecurity Law*:** The National Peoples' Congress (NPC) released the second draft Cybersecurity Law that would create a firmer legal basis for regulating the activities of the Cyberspace Administration of China (CAC), impose a variety of obligations on "network providers," impose additional security and testing requirements and security "reviews" on certain software and IT products and services, limit international data flows, and establish a prescriptive personal data protection regime.

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.

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: Several agencies under the State Council, the National Development and Reform Commission (NDRC), the State Administration of Industry and Commerce (SAIC), and the Ministry of Commerce (MOFCOM) are in the process of developing rules regarding the abuse, or misuse, of intellectual property rights (IPR) under the Anti-Monopoly Law (AML). BSA members remain concerned that there may be divergent approaches to AML-enforcement regarding IPR, enhancing business uncertainty and exposing rights holders to administrative abuse or allowing 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

[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

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 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 these objectives, 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) issued draft Regulations on the Protection of Personal Data in Electronic Systems in July 2015. The draft regulations, which are still pending, raise 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.

[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).

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 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 September 2016, the regulation was still pending.

JAPAN

Overview:

Japan is considering privacy rules and has adopted security measures that may inadvertently restrict data flows and create barriers to trade without improving data privacy or security. A flexible and objectives-oriented approach to privacy that avoids overly prescriptive rules, unnecessary administrative compliance requirements, and Japan-specific standards that diverge from internationally accepted standards and practices should be adopted. In addition, a risk-based approach to cybersecurity that allows government agencies to maximize security and utilize cloud-based productivity and service solutions should be sought.

Specific Concerns:

***Privacy*:** The amended Personal Information Protection Act (PIPA) creates obligations that may impose unnecessary burdens on the operation of BSA members and create market access barriers, such as overly strict requirements regarding user consent and restrictions to cross-border data flows. The Personal Information Protection Commission (PPC) is currently developing PIPA-implementing regulations. BSA acknowledges and appreciates the significant efforts by the Government of Japan (GOJ), and the PPC in particular, to reach out to stakeholders, including global industry bodies, to solicit input before issuing final draft regulations. Restriction of data flows would be very trade disruptive and BSA urges the US Government to continue working with the GOJ to avoid this outcome.

Cybersecurity: Japan has updated legislation and developed a variety of policies to enhance the cybersecurity capabilities of government agencies and industry. Although many of the changes are positive, there are measures (such as recommendations to physically separate government networks from the Internet) that are likely to deter the adoption of valuable Internet-enabled services (such as cloud computing) by government agencies and the private sector. This would represent a barrier to US companies wishing to provide Internet-enabled services in Japan.

REPUBLIC OF KOREA

Overview:

The overall commercial environment in the Republic of Korea (Korea) for BSA members, and the software and IT sector as a whole, is mixed. Korea has a strong IT market and a mature legal and enforcement system. Over the last several years, however, a number of policies have been adopted that have erected substantial market access barriers to foreign software and IT products. Such policies include limits to the use of commercial cloud services by public sector entities and other regulated sectors; local testing requirements; and requirements to comply with national technical standards even when commonly used international standards are available.

Specific Concerns:

Cross-Border Data Flows and Server Localization: Although the Cloud Computing Promotion Act came into force as of September 28, 2015, the National Intelligence Service (NIS) has maintained the position that public sector entities should not use commercial cloud services without following specific NIS guidelines, including the requirement that internal systems be physically separated from public-facing systems. Similar guidelines and regulations requiring network separation and/or data localization exist for the finance and healthcare sectors. We are concerned that, even after enactment of the Cloud Computing Promotion Act, significant barriers still exist to cloud service adoption.

Discriminatory Security Certification Requirements Applied for Foreign IT Products: Since 2011, the Korean government has imposed additional security verification requirements for international Common Criteria-certified information security products that are procured by Korean government agencies. However, no such requirement is applied to locally-certified products. In 2014, the Korean Government extended similar security-conformity testing requirements to international Common Criteria-certified networking products for all central government agencies. In 2016, the government is expected to further extend the policy to all public organizations, local governments, and other government-related agencies, such as educational institutions. In combination, Korean government agency procurement authorities may be interpreting these policies as requirements to buy local IT products and to avoid foreign products, although we are unaware of any such interpretation has been reduced to writing. While the Korean Government has issued clarifications to government agencies, to date there has been no change in the implementation of these policies.

Korea is a member of the Common Criteria Recognition Arrangement (CCRA) and therefore should recognize international certification from accredited laboratories and should not impose further requirements for certified products. The additional requirements are not consistent with the spirit of CCRA, which is to “eliminate the burden of duplicating evaluation of IT products and protection profiles.” To make matters worse, separate conformity testing is required for each government agency, even if it is the same product that has been procured and verified for another government agency.
This discriminatory application of security testing in public procurements to only international information security products also appears to be inconsistent with Korea’s international commitments to national treatment and non-discrimination, including in the U.S.-Korea Free Trade Agreement.

While the Korean Government has indicated that they intend to change the policy, they have yet to issue any formal correction in writing. This has resulted in confusion as to what the applicable requirements are. Although BSA and other organizations have raised this issue several times with the Korean Government, the issue remains unresolved at this time.

THAILAND

Overview:

BSA is concerned that fair and equitable market access for our members' products and services could be harmed if legislation regarding personal data protection and cyber security remains both vague and potentially over-prescriptive. BSA appreciates the opportunities to discuss and address concerns in these bills with the Royal Thai Government (RTG) and we urge these concerns be addressed before the bills are finalized.

Specific Concerns:

***Security*:** The Ministry of Information and Communication Technology (MICT), now the Ministry of Digital Economy and Society (MDES), is reviewing the draft National Cybersecurity Bill. The draft bill is designed to strengthen the cybersecurity capabilities of government agencies and provide appropriate breach notification procedures. However, it raises concerns because it would give the Office of the National Cybersecurity Committee broad powers to access confidential and sensitive information without sufficient protections to appeal or limit such access. Granting the Office of the National Cybersecurity Committee such broad powers will undermine public confidence and trust in IT generally and harm the ability of BSA members to provide the most innovative and effective software solutions and services to the market in Thailand.

***Privacy*:** The draft Personal Data Protection Bill (PDP Bill) is also under review by the MDES. The PDP Bill is designed to build public trust and confidence in IT products and services and to implement the APEC Privacy Framework's principle of cross-border data transfer. BSA filed comments on the draft legislation in March 2015 and held a number of meetings with the RTG, where we highlighted the importance of protecting personal information and preventing misuse of such information for fostering the trust and confidence necessary for growth of the digital economy. However, BSA notes that the draft PDP Bill contains imprecise or unclear provisions in some cases, and in others appears to take an overly prescriptive approach that does not adequately take into consideration the nature of the personal information in question. Such an approach is not consistent with the expected technical and commercial evolution of digital products and services, and could result in undermining both the effective protection of personal information and the trust and confidence that are necessary for widespread adoption of digital products and services in the economy.

VIETNAM

Overview:

Vietnam has enacted and/or proposed a number of laws or regulations that will likely impose restrictions on the cross-border transfer of data or require server localization in Vietnam. These measures not only hamper the ability of BSA members and others in the IT sector to provide innovative products and services to the Vietnamese market, but they may also conflict with commitments to allow the cross-border transfer of information by electronic means under the Trans-Pacific Partnership (TPP).

Specific Concerns:

Information Security: Vietnam's legislative body, the National Assembly, enacted the Law on Network Information Security in December 2015. The law has been in force since July 1, 2016. BSA's concerns with the law and several implementing rules include obligations to disclose proprietary information as a condition to enter the market, overly broad definitions of personal information, and overly broad provisions requiring "cooperation with the Government" regarding access to data and requirements to decrypt encrypted information held by third parties. These provisions impact the ability of BSA members to provide services in Vietnam and appear to conflict with Vietnam's international commitments in the TPP.

Cross-Border Data Flows and Server Localization: On September 1, 2013, Decree No. 72 went into effect.[6] The decree imposes onerous requirements on server localization and restrictions to cross-border data flows that will undermine the ability of BSA members to provide digital services in Vietnam. Specifically, Article 4.2.f of Circular No. 9, which implements certain provisions of Decree No. 72, requires general news website operators, social network service providers, search engines, and online applications to have at least one server system in Vietnam to allow for inspection, storage, and provision of information at the request of competent authorities.[7] In early 2015, the Government of Vietnam proposed to further elaborate these requirements in a draft circular. The draft circular also mandates companies providing certain online services to establish a local entity in Vietnam. These measures may impact the ability of BSA members to provide software-based services online (e.g., cloud computing), which offer many economic benefits, especially to small- and medium-sized enterprises in Vietnam. The 2015 Draft Circular has not yet been finalized.

[6] Decree No. 72 72/2013/ND-CP on the Management, Provision, and Use of Internet Services and Online Information

[7] Ministry of Information and Communication's Circular No. 09/2014/TT-BTTTT: Detailing management, provision and use of information on websites and social networks (in force since October 3, 2014)

EUROPE

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 are extremely trade disruptive, as the ability to transfer data internationally is the lifeblood of the digital economy. US companies currently face a great deal of uncertainty regarding the legal mechanisms relied upon to transfer data out of the EU. The US-EU Privacy Shield, which replaced the former Safe Harbor transfer mechanism, took effect on August 1, 2016, and will be reviewed in mid-2017. Many European data protection authorities and members of European Parliament continue to resist the new agreement, and a judicial challenge to it is likely.

In addition, the use of Standard Contractual Clauses, another 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 European Court of Justice in 2017. Further, the European Commission later this year is expected to release a legislative proposal on data flows among EU member states, which likely will not impede data localization measures proliferating among member states (see entries on France and Germany below). Next year, the European Commission may also propose new rules on data ownership, portability, and interoperability that could disrupt the data value chain and negatively affect the added value of BSA members' products. These developments collectively create a volatile environment which impedes the ability of US companies to do business in the EU.

General Data Protection Regulation (GDPR) Implementation: The GDPR was adopted in April 2016 and will apply across the EU in May 2018. Data protection authorities and the Commission are expected to issue a number of implementing measures during the 2016-2018 transition period. However, the Data Protection Authorities do not plan 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 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. TDM performed on lawfully accessed works neither conflicts with the normal exploitation of such works nor undermines the legitimate interests of authors. Nevertheless, the European Commission has proposed a digital copyright directive that would cast a pall on innovation by creating uncertainty about the legality of TDM under the existing copyright framework. Because the Commission's proposed TDM exception would apply only to public interest research organizations engaged in scientific research, it could create an implication that such activity, when performed by commercial entities, falls outside of the existing

temporary copy exception. Legal certainty about TDM is critical to the investment in data analytics research and development. 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.

Digital Content Directive: The proposed Digital Content Directive would introduce potentially burdensome rules with respect to the supply of digital content, including software and cloud services. 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 in the course of providing online services (e.g., quality assurance data, telemetric data, and cybersecurity data). Ongoing discussions regarding the Digital Content Directive could also result in re-classification of software embedded in consumer devices as "goods," thereby exposing companies to increased liability for consequential damages.

Cybersecurity Contractual Public-Private Partnership (cPPP): Earlier this year, the European Commission launched a cPPP initiative on cybersecurity aimed at fostering cooperation between public and private actors at early stages of the research and innovation processes in order to provide access to innovative and trustworthy European solutions by Europeans. However, in order to participate in the cPPP (including participating in public procurement), a company would have to 1) be an EU-headquartered company; and 2) spend a significant part of its research and development in the EU. Should this initiative remain unchanged, it would pose a competitive disadvantage to US companies wishing to participate in the public procurement of cybersecurity products and services in the EU.

GERMANY

Public Procurement of Cloud Services: In July 2015, the Federal Government IT Advisory Committee issued new criteria for all prospective cloud (SaaS, PaaS, IaaS) vendors to German Federal agencies, including the localization of sensitive data, the ability for the Federal agencies to "ensure that security controls can be met" – possibly leading up to a mandatory request to disclose sensitive commercial information (e.g. source-codes), and preference for state-owned companies unless they do not provide the preferred service. These requirements pose a significant barrier to US companies wishing to provide cloud services in Germany.

UNITED KINGDOM

Investigatory Powers Bill: The UK Government is seeking to advance a bill in Parliament to regulate the government's investigatory powers before existing legislation on data retention expires at the end of 2016. Major concerns regarding the bill include: broad powers to demand the removal of encryption and require system redesign; extraterritorial scope of equipment interference powers and hacking obligations; expanded types of companies and services subject to surveillance; bulk data collection through interception and other means; and broader data retention obligations. If these concerns are not addressed, the bill will impose significant barriers to companies rendering information technology services in the United Kingdom.

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:

Privacy Legislation: 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.

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 by October 9, 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.