October 30, 2018

Docket No. USTR-2018-0029

Edward Gresser
Chair of the Trade Policy Staff Committee,
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Dear Mr. Gresser,

BSA | The Software Alliance[1] provides the following information pursuant to your request (83 Fed. Reg. 42966, August 24, 2018) for written submissions to the Trade Policy Staff Committee (TPSC) regarding significant barriers to US exports of goods and services and US foreign direct investment for inclusion in the NTE Report.

Software has a profound impact on the American economy. The US software industry — and millions of American researchers, engineers, and other workers employed in this industry — benefit from American global leadership in the development and provision of software services, including cloud computing services, data analytics, machine learning, cybersecurity solutions, and more. In 2016, the software industry was responsible for $1.14 trillion of total US value added GDP. The industry supported 2.9 million jobs (directly) and 10.5 million jobs (indirectly) — jobs that pay significantly higher than the national average for all occupations.[2] US exports of telecommunications, computer, and information services (including software) totaled more than $42 billion in 2017. This economic progress, coupled with more than $63 billion 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 foreign government measures — hampering US business models and hindering the international movement of data. The transformation of data services and digital delivery models provides tremendous benefits to users. This ability to move data across borders is critical to both the business offerings and core operations of enterprises that make up the digital economy.

[1] BSA's members include: Adobe, Akamai, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] Software.org, The Growing $1 Trillion Economic Impact of Software (Sept. 2017), available at: https://software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

Section 181 of the Trade Act of 1974, as amended (19 USC 2241) requires the United States Trade Representative (USTR) to "identify and analyze acts, policies, or practices of each foreign country which constitute significant barriers to, or distortions of—

- United States exports of goods or services (including … property protected by trademarks, patents, and copyrights exported or licensed by United States persons);
- foreign direct investment by United States persons, especially if such investment has implications for trade in goods or services; and
- United States electronic commerce."

It also requires USTR to make estimates of the economic impact on US commerce resulting from such acts. USTR's solicitation of comments sought input on, among other things:

- Trade restrictions implemented through unwarranted standards, conformity assessment procedures or technical regulations (technical barriers to trade);
- Government procurement restrictions (e.g., ''buy national policies'' and closed bidding);
- Lack of intellectual property protection;
- Barriers to trade in services (e.g., prohibitions or restrictions on foreign participation in the market, discriminatory licensing requirements or regulatory standards, local presence requirements, and unreasonable restrictions on what services may be offered);
- Barriers to digital trade (e.g., barriers to cross-border data flows include data localization requirements, discriminatory practices affecting trade in digital products, restrictions on the provision of Internet-enabled services, and other restrictive technology requirements);
- Investment barriers (e.g., limitations on foreign equity participation and on access to foreign government-funded research and development programs, local content requirements, technology transfer and export performance requirements, and restrictions on repatriation of earnings, capital, fees, and royalties); and
- Government-tolerated anticompetitive conduct of state-owned or private firms that restrict the sale or purchase of US goods or services in the foreign country's markets.

In this submission, we address all three statutory elements of Section 181 of the Trade Act, and to the extent possible, we address each of the areas identified in USTR's Federal Register notice as they relate to BSA members' challenges faced in partner markets. In the introductory sections below, we describe BSA's Digital Trade Agenda and market access challenges in select economies.

BSA's Digital Trade Agenda

BSA supports trade-related initiatives and legal frameworks at home and abroad that are conducive to the development of digital trade and e-commerce, and that will allow for the emergence of new digital technologies. BSA's Digital Trade Agenda is supported by four major pillars: Data Economy, Regulation, Intellectual Property, and Technology in Government.[3] In each of these areas, it is critical for policymakers to be vigilant against the creation of trade barriers and disguised restrictions on trade, and to use all of the trade tools possible to push for the removal of such barriers and restrictions wherever they exist.

[3] Comments available at https://www.bsa.org/~/media/Files/Policy/Trade/2017BSATradeAgendaGlobal.pdf

Market Access Challenges in Select Economies

Cross-border data flows: The ability of US companies to continue leading global advances in innovative technology is under a rising threat from foreign government policies that hamper US business models and hinder the international movement of data. Cross-border data flows are key to the current and future success of the US economy, and will only grow more important in the coming years. Barriers to cross-border data flows are often disguised as privacy or security measures. Immediate attention to these threats is urgently needed. Unfortunately, a number of markets, including **Brazil, China, India, Indonesia, and Vietnam**, 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 monitoring developments in the **EU** that could pose significant barriers to providing digital services in that market.

Data-related market access barriers take many forms. Sometimes they expressly require data to stay in-country or impose unreasonable conditions in order to send it abroad. In other cases, they require the use of domestic data centers or other equipment. Sometimes the barriers are based on privacy or security concerns, but too often the real motivation is protectionism, as the means chosen tend to be significantly more trade-restrictive than necessary to achieve any legitimate public policy goal.

Due to the trade-disruptive impact of measures that impede cross-border data flows and mandate data localization, BSA urges the US Government to work with its trading partners to prevent or remove such practices. All available trade mechanisms should be leveraged for this purpose.

Procurement Restrictions: Governments are among the biggest consumers of software products and services, yet many are imposing significant restrictions on foreign suppliers' ability to serve public-sector customers. Not only do such policies eliminate potential sales for BSA members, but they also deny government purchasers the freedom to choose the best available products and services to meet their needs. US trading partners with existing or proposed restrictions on public procurement of foreign software products and services include **Brazil, China, India, Indonesia, and Vietnam.**

Security: Governments have a legitimate interest in ensuring software products, services, and equipment deployed in their countries are reliable, safe, and secure. However, a number of countries are using or proposing to use security concerns to justify *de facto* trade barriers. Such countries include **Brazil, China, Korea, Thailand, and Vietnam**. Furthermore, other countries do not allow government agencies to procure cloud services from companies that store data outside the country, citing security concerns. Requiring cloud service providers to confine data in-country does not improve security, but hampers it, as it prevents data from being backed up in multiple locations. Data security is ultimately not dependent on the physical location of the data or the location of the infrastructure supporting it. Rather, security is a function of the quality and effectiveness of the mechanisms and controls maintained to protect the data in question.

Standards: Technology standards play a vital role in facilitating global trade in IT. When standards are developed through voluntary, industry-led processes and widely used across markets, they generate efficiencies of scale and speed the development and distribution of innovative products and services. Unfortunately, a number of countries have developed or are developing country-specific standards to favor local companies and protect them against foreign competition. This creates a *de facto* trade barrier for BSA members, raises the costs of cutting-edge technologies to consumers and enterprises, and places the domestic firms these policies are designed to protect at a disadvantage in the global marketplace. Countries adopting nationalized standards for IT products include **China, India, Korea, and Vietnam**.

Intellectual Property Challenges in Select Economies

Patents: BSA members invest enormous resources to develop cutting-edge technologies and software-enabled solutions for businesses, governments, and consumers. It is therefore critical that countries provide effective patent protection to eligible computer-implemented inventions, in line with their international obligations. Some countries have adopted or are considering policies that could significantly

constrain the freedom of patent holders to negotiate licenses for their inventions. For example, **China** has proposed a variety of policies that could unfairly restrict the ability of patent holders to exercise their legitimate rights to enforce their patents or to negotiate mutually acceptable licensing terms.

Trade Secrets and Other Proprietary Information: BSA members also rely on the ability to protect valuable trade secrets and other proprietary information to maintain their competitive position in the global marketplace. US trading partners that fail to implement and enforce strong rules protecting trade secrets against misappropriation or unauthorized disclosure put BSA members' business operations at risk and prevent them from having legal recourse when misappropriation or unauthorized disclosure occurs. Given the ease by which such information can be transmitted, this presents serious market challenges not only in the specific country in question, but also globally. Current or proposed policies that require the disclosure of sensitive information as a condition for market access represent enormous market access barriers for BSA members. Countries with weak trade secret protection rules, or that have or are proposing policies requiring disclosure of sensitive information include **China, India, and Indonesia.**

Conclusion

BSA welcomes the opportunity to provide this submission to inform the development of the 2019 National Trade Estimate and the US Government's engagement with important trading partners in 2019. We look forward to working with USTR and the US agencies represented on the TPSC to achieve meaningful progress in addressing the barriers to trade, investment, and e-commerce identified in this submission.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

TABLE OF CONTENTS

CHINA

Overview/Business Environment

BSA members and other foreign technology providers face a particularly challenging commercial environment in China.[4] In 2017 and 2018, the Government of China issued numerous policies and standards designed to implement the Cybersecurity Law.[5] The law raises significant market access challenges for US and other foreign software and IT companies related to data localization, security, and privacy which could be exacerbated or mitigated depending on how the implementing measures (many of which are still in draft form) are finalized. In addition, various government agencies have proposed sector-specific cybersecurity regulations that require firms to replace existing IT systems with "secure and controllable" products and services. The term "secure and controllable" is associated with a number of vague or unreasonable requirements and has been frequently interpreted by regulated entities as an instruction from the government to procure domestic products and services.

Beyond cybersecurity, China's regulatory regime also makes it extremely difficult for BSA members to participate in the digital market. China has proposed further restrictions to the existing system, which already effectively excludes foreign participation in cloud computing and other data services in China. While there have been some openings in the electronic commerce field, China continues to regulate Internet and cloud computing services as value-added or basic telecommunications services (VATS or BTS) 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. BSA urges the US Government to continue to closely engage with the Government of China to make meaningful progress on the range of issues mentioned in this submission to ensure fair and equitable market access for BSA members and other US and foreign companies.

Market Access

BSA seeks a fair and level playing field for competition in the software and related technologies market. Market access restrictions are often imposed under the guise of ensuring the security of government systems and important economic sectors. While these are important priorities for all countries, the challenge is to ensure that security-related policies are not used as a pretext for adopting measures that act as unnecessary and illegal barriers to market access. Furthermore, market access for software and other IT products and services should not be limited to those with IP that is locally owned or developed, nor should it depend on the transfer of IP to domestic firms.

Cybersecurity Law: In November 2016, the National Peoples' Congress passed the Cybersecurity Law (CSL), which went into effect in June 2017.[6] The law imposes a variety of obligations on "network providers"; imposes additional testing requirements on the procurement of certain software and services for "Critical Information Infrastructure" (CII) operators; limits international data transfers; and establishes a prescriptive personal data protection regime. Since early 2017, the Cyberspace Administration of China (CAC) and other authorities have been issuing measures and standards to implement the law. Many of these measures leave important issues vague and unclear (e.g., the definition of CII or "important information"), or appear to expand the scope of the law exacerbating the negative impact of these rules on the software industry

[4] AmCham China: China Business Climate Survey Report, at http://www.amchamchina.org/policy-advocacy/business-climate-survey/; *See generally,* BSA Cloud Scorecard – 2018 China Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_China.pdf

[5] China Cybersecurity Law (2016) (Chinese) at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

[6] Ibid.

(e.g., requiring that personal information and important information collected in China, and not just by CII operators, must be held in China).

The expansive regulatory mandate advanced by the CSL has resulted in the emergence of numerous administrative initiatives to strengthen the government's role in managing networks, services, and data across nearly every sector of the Chinese economy. One prominent example of this can be seen in a July 2018 notice released by the People's Bank of China (PBOC) that aims to tighten management of cross-border financial networks and information services. This notice could empower Chinese government agencies to require that overseas providers procure and use certified or tested network critical equipment and cybersecurity products, use encryption products approved by the China State Cryptography Administration (SCA), and tolerate government supervision and surveillance of cross-border data transfers.

Cybersecurity Classified Protection Regulation: On June 27, 2018, China officially established a cybersecurity protection baseline for network operators and a universal compliance framework for the CSL by releasing the draft Cybersecurity Classified Protection Scheme (CCPS) — a continuation of the Multi-level Protection Scheme (MLPS) jointly established by MPS, the State Encryption Management Bureau (SEMB), the Ministry of State Security (MSS), and the State Council Information Office (SCIO) in 2007. Like MLPS, CCPS ranks the importance of network and information systems, based on their importance to China's national security, social order, public interests, and the legitimate interests of individuals and organizations, on a scale from 1 to 5, with Level 5 constituting the most sensitive to national security interests.

Similar to China's draft implementation regulations for CII, the Draft CCPS also imposes several significant requirements regarding the structure and maintenance of networks operating within China. For instance, the CCPS would requires that systems at Level 3 and above must be connected with China's Public Security Bureau (PSB) system (managed by MPS) and stipulates that all technical maintenance performed on networks must be localized. These unnecessarily intrusive requirements threaten to shut foreign technology out of systems ranked at CCPS Level 3 and above, constituting a significant point of concern for the industry at large.

Encryption: Over the past few years, the China National Information Security Standards Technical Committee (TC-260) has released a myriad of draft cybersecurity standards involving encryption for public comment. A consistent and worrying trend exhibited by these standards is that they de facto replace all international algorithms and schemes with domestic ones. Such changes to algorithms or encryption mechanisms create technical barriers to trade and undermine interoperability.

A 1999 commercial encryption regulation deemed all commercial encryption products as "state secrets" and prohibited the use of foreign encryption products. Unless companies can demonstrate that the 'core function' of the products they wish to sell are not encryption, then the product is banned from the Chinese market. Additionally, the State Commercial Cryptography Administration (OSCCA) requires companies to turn over source code and other proprietary information for testing by state laboratories in order to gain market access for certain encryption products.

More recently, in April 2017, SCA published a draft Encryption Law for public comment. The draft law is concerning for several reasons. First, it would fully or partially bar foreign competition in various categories of cryptography. Of the three categories defined by the law (core, common, and commercial cryptography), foreign businesses would only be allowed to participate in the commercial cryptography market, and even then only under strict regulations. Additionally, the draft law lacks a clear definition of the scope of commercial cryptography, leaving significant uncertainty about which products and services foreign companies might provide. And finally, the licensing scheme for foreign commercial cryptography providers, as envisioned by the draft law, would require such providers to disclose source code to state licensers, putting their IP at significant risk.

Cyber Critical Equipment and Cybersecurity Specific Product Catalogue: The Catalogue of Network (Cyber) Critical Equipment and Cybersecurity-Specific Products (Batch 1) was jointly released by CAC, the Ministry of Industry and Information Technology (MIIT), MPS, and the Certification and Accreditation

Administration (CNCA) on June 9, with retroactive effect from June 1, 2017 without a comment period or consultation with industry. The Catalogue introduces a market-entry requirement for the equipment and products in the catalogue, mandating they be certified or tested in accordance with the mandatory requirements of relevant national standards before entering the market, as well as Chinese standards and "other mandatory requirements," which remain unspecified at this time. It is not clear whether such requirements will be aligned with applicable international standards and be consistent with the World Trade Organization Agreement on Technical Barriers to Trade (TBT Agreement) obligation that technical regulations follow international standards where such standards exist.

Restrictions on Cross-Border Data Transfers: The Government of China has put in place a number of laws and regulations restricting the free flow of data across borders and forcing data to be stored locally. For BSA members that provide cloud computing services or that rely heavily upon cloud computing for their business operations, these restrictions create an uneven playing field — advantaging domestic businesses that already have local infrastructure and preventing foreign businesses from operating efficiently or at all. Below, we summarize key laws and regulations impeding cross-border data flows.

The Cybersecurity Law requires "personal information and other important data gathered or produced by critical information infrastructure operators during operations" to be stored within China. In 2017, the CAC issued draft Critical Information Infrastructure Protection regulations that contain an exceptionally broad definition of "critical information infrastructure" that would include cloud computing services.[7] These regulations, if enacted as drafted, would effectively require all cloud computing services providers (CSPs) operating in China to store data from their operations in China, thus creating additional operational costs and access challenges for foreign providers.

In April 2017, the CAC issued draft Security Assessment Measures for Cross-Border Transfers of Personal Information and Important Data for public comment. The draft measures contain obligations relating to security assessments, impose additional localization requirements and restrictions on the transfer of "personal information" and "important data" across borders, and restrict remote access to such data stored in China from outside its borders. The draft measures — if adopted in their current form — create unacceptable legal risk for CSPs dependent on cross-border data flows for their business operations and will serve as another key barrier to digital commerce.

Cloud Market Access: Cloud computing, despite being identified as an area of strategic development in China, remains largely off limits to foreign ICT companies due to several policy challenges, including equity caps, investment restrictions, and connectivity requirements. These challenges are exacerbated by market entry barriers, such as restrictions on the ability to engage in cross-border data transfer and requirements to localize computing infrastructure.
In November 2016, MIIT published a Draft Notice on Regulating Business Operation in Cloud Services Market (Draft Cloud Service Regulation Notice). BSA and other associations submitted comments to the Government of China raising concerns about the Draft Cloud Service Regulation Notice and its implications for the operation of foreign cloud computing businesses in the country.[8]

While the Draft Cloud Service Regulation Notice has not yet been finalized, it contains several provisions that would serve as highly problematic market barriers to foreign CSPs. These include provisions that, among other things, require CSPs to physically construct and maintain infrastructure in China; subject cross-border data transfers to a range of restrictions; limit the ability of foreign companies to market their services in China under their own brand; and create duplicate copies of equipment, business systems, and data. This potentially makes it cost-prohibitive and operationally impractical for foreign CSPs to operate in China, preventing them from participating on equal terms within the Chinese market and impeding their ability to partner on reasonable terms with Chinese companies.

[7] Draft Critical Information Infrastructure Protection Regulations (2017) (Chinese) at http://www.cac.gov.cn/2017-07/11/c_1121294220.htm

[8] Comments available at https://www.bsa.org/~/media/Files/Policy/Trade/CloudRegComments.pdf

Finally, while these policies themselves create specific concerns, particularly in relation to licensing requirements that bar foreign businesses from competing in China on equal terms as domestic entities, the implementation of these policies can be equally concerning, and far more difficult to document. BSA members attempting to provide cloud computing or other VATS must navigate a licensing process that can be lengthy, unpredictable, burdensome, and discriminatory. Businesses have encountered requirements or pressure to disclose IP and have dealt with inconsistent interpretation of regulations between central and local regulators, lengthy or open-ended approval timelines, and a lack of transparency around decision-making while navigating the licensing process. These concerns represent a significant barrier to foreign access to the Chinese market.

Procurement: In May 2017, the CAC issued the Interim Measures for the Security Review of Network Products and Services.[9] Under the measures, all "important network products and services" purchased for national security-related networks and information systems will be subject to review by third-party assessors operating under the auspices of a cybersecurity review office, to be established by the government. The measures do not define "important network products and services" or delineate what systems are national security related. They also fail to specify how the third-party assessors will be designated, the steps that an applicant should follow to have products or services reviewed, or what remedies are available for any wrong decisions made by the cybersecurity review office. BSA and its members remain concerned that the measures and the review process will be used as a disguised market access barrier to foreign products and services.

There are also long-standing procurement measures in place, such as the MLPS. The MLPS, and its proposed successor scheme the CCPS, impose 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 IP owned in China. This applies to procurements by the government and increasingly to procurements by state-owned enterprises (SOEs) and the private sector, restricting market access for foreign information security products. As a result, many entities in China are unable to procure the most effective software and security tools to meet their needs.

Foreign Direct Investment Restrictions: US businesses seeking to operate in China are subject to a range of foreign direct investment restrictions, including equity caps, investment restrictions, in-country hosting requirements, and similar regulations, as well as challenging processes for obtaining licenses and other prerequisites for entering the market. These restrictions are particularly acute for the telecommunications and IT industries, including Cloud computing services.
In March 2016, a new Telecom Service Catalog went into effect, expanding the scope of China's telecoms regulation and imposing a host of associated market access restrictions on foreign firms, which are not typically regulated as telecom in the rest of the world. The measures incorrectly classify a wide range of technologies and services as VATS or BTS, when in fact they are computer or business services that utilize the public telecom network as a method of delivery. For example, the catalog classifies cloud computing, content delivery networks, and online interactive platforms (called information services) as telecommunications services. Foreign firms that provide value-added services in China can only operate through joint ventures, of which they may own no more than 50 percent for VATS and 49 percent for BTS. In short, because of the update, foreign firms that provide a range of IT services are now subject to explicit limitations on market access and, indirectly, mandatory technology transfer to the local partners of joint ventures.

[9] Interim Measures for the Security Review of Network Products and Services (2017) (Chinese) at http://www.cac.gov.cn/2017-05/02/c_1120904567.htm

Intellectual Property

Intellectual Property and Competition: Prior to the establishment of the consolidated regulatory body — the State Administration for Market Regulation (SAMR) — several agencies under the State Council, the National Development and Reform Commission (NDRC), the State Administration of Industry and Commerce (SAIC), the Ministry of Commerce (MOFCOM), and the State Intellectual Property Office (SIPO) were in the process of developing rules regarding the abuse, or misuse, of IP under the Anti-Monopoly Law (AML). BSA members remain concerned that there may be divergent approaches to AML enforcement regarding IP — increasing business uncertainty, exposing rights holders to administrative abuse, and allowing agencies to use AML enforcement for industrial policy or other protectionist purposes. Specific concerns include applying rules tailored to standard-essential patents (SEPs) 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 IP rights.

In November 2017, China passed a revised Anti-Unfair Competition Law (AUCL), which took effect on January 1, 2018.[10] BSA members are concerned about the broad definition of "unfair competition" in the AUCL and the overlap with the AML. More recently, on March 29, 2018, the State Council released the Measures for Transfer of Intellectual Property Rights to Foreign Investors (Trial) with an aim to implement a holistic view of national security, improve China's national security system, and regulate the transfer of intellectual property rights to foreign investors. According to the Measures, matters subject to review include patents, integrated circuit layout designs, computer software copyrights, new plant varieties, and the right of application thereof. The review measures proposed by this legislation raise significant concerns for foreign investors surrounding IP protection, and introduce considerable regulatory interference in commercial affairs.

In addition, technology businesses are subject to insufficient and contradictory laws relating to contracts and liability for infringement. China's Contract Law generally permits contracting parties to negotiate on who will bear the liability for infringing products. However, for technology import and export contracts, the Contract Law states that the position under the Technology Import and Export Regulations will apply instead — where technology importers must indemnify their customers and bear the liability for infringing products. This lack of freedom to contract discriminates against overseas licensors and could be viewed as a non-tariff technical barrier.[11]

Source Code and Enterprise Standards Disclosure Requirements: Through a series of draft and final legislative documents, the Government of China has made clear its intention to establish a legal basis for requiring the disclosure of source code and enterprise standards associated with foreign software products across a wide range of uses. Requirements for the disclosure of source code and enterprise standards pose significant inherent risks to IP, with little security value. It is critical that the US Government intervene to eliminate current disclosure requirements and arrest further advancement of draft requirements.

The most significant measure relating to source code disclosure is China's Cybersecurity Law, which includes requirements that products associated with CII be subject to security reviews. Current implementing measures under the law contemplate that source code disclosures can be required as part of the security reviews but leaves the mechanism of this to future legislation. The possibility of such mandated source code disclosures is cause for substantial concern among BSA members and other US companies. Additionally, as mentioned above in the area of cryptography, foreign commercial

[10] Anti-Unfair Competition Law (2017) (Chinese) http://www.npc.gov.cn/npc/xinwen/2017-11/04/content_2031432.htm\

[11] The United States and the European Union have initiated WTO dispute settlement proceedings against China with respect to these Regulations and related measures. *See China – Certain Measures Concerning the Protection of Intellectual Property Rights,* Request for Consultations by the United States, WT/DS542/1 (March 26, 2018); *China – Certain Measures Affecting the Transfer of Technology,* Request for Consultations by the United States, WT/DS549/1 (June 6, 2018).

cryptography providers would be required to disclose source code to state licensers under the SCA's draft Encryption Law.

Equally concerning are revisions that China enacted to the Standardization Law on November 4, 2017. The revised law appears to require public disclosure of enterprise standards (which are described as an individual company's proprietary product or services specifications). Enterprise standards represent highly proprietary and confidential information that often is protected by trade secret law or other forms of IPR.[12] Their public disclosure would prove exceptionally damaging to the integrity of IP held by US technology companies.

In July 2018, SAMR, NDRC, the Ministry of Science and Technology (MOST), MIIT, and four other government bureaus released Opinions on Implementing a Pioneer System for Enterprise Standards. This system of ranking standards hand-picked by the government conditions access to government incentives on enterprises' meeting onerous disclosure requirements, including standards implemented, levels of standards on the platform, functional indicators of their products or services, and performance indicators of products. No other country in the world requires public disclosure of comprehensive lists of technical standards used in products or services. Not only would such disclosure compromise valuable IP, but it would also establish a significant cost burden on businesses.

[12] China does not currently have a standalone trade secrets law, and trade secrets remain one of the most at-risk types of intellectual property for US businesses operating in China. While companies do have legal recourse to pursue cases of trade secrets violations, existing procedures make it difficult for victimized businesses to achieve any favorable legal resolution. The most significant challenge is the difficulty companies face under the Chinese court system in establishing a valid and effective evidence chain due to the complexity of evidence rules and rules governing the burden of proof. It is critical that China develop a standalone trade secrets law to afford adequate protections to foreign businesses, provide clear and fair rules regarding evidentiary chains and burden of proof, and ensure sufficient enforcement.

INDIA

Overview/Business Environment

The commercial environment for BSA members remains challenging in India.[13] In addition to certain policy and regulatory developments that may require data localization and impact cross-border data flows, the preference for domestic products and services contained in certain procurement policies could restrict market access for BSA members.

The Committee of Experts[14] (Expert Committee) on Data Protection under the Chairmanship of Justice B. N. Srikrishna (former Judge, Supreme Court of India) submitted its Data Protection Committee Report (Report)[15] and the Personal Data Protection Bill, 2018 ('Bill')[16] to the Ministry of Electronics and IT (MeitY) in July 2018. This Bill has seen extensive debate, as it includes contentious provisions such as personal data localization requirements and restrictions on the cross-border transfer of personal data. In parallel to this important policy development, various government bodies and regulators, including the Reserve Bank of India (RBI), have demonstrated an intent in their support for data localization requirements.

Government procurement policies remain outmoded and inefficient because of local content and technology preferences. Most recently, the Department of Industrial Policy and Promotion (DIPP) issued the Public Procurement Order 2017 (Make in India Order), which requires government departments to give preference to local suppliers in procuring goods and services.[17] In addition, the Draft National Policy on Software Products would promote the use of domestically developed software products in public sector procurements and strategic sectors like defense, telecom, power, and healthcare.[18] Such policies do not offer a level playing field to US technology providers, who are bringing cutting-edge technologies and services to India.

The existing and future software market in India also remains at risk due to a variety of existing or proposed data localization requirements. From legacy policies on government-owned weather data, to proposals regarding machine-to-machine (M2M) systems, payment processing, and existing public procurement requirements, the Government of India appears to be considering requiring the localization of data sets within India for a variety of reasons. These policies do not promote security. Rather, they unfairly disadvantage firms that provide or rely on global cloud computing services.

Market Access

The Government of India, at the central and state levels, has adopted a variety of policies affecting the commercial environment for BSA members and the information technology (IT) sector in general.

---

[13] *See generally*, BSA Cloud Scorecard – 2018 India Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf

[14] The Committee of Experts on Data Protection (2017) at http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf

[15] Data Protection Committee – Report (2018) at http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf

[16] Personal Data Protection Bill (2018) at http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

[17] Public Procurement Order 2017 (Make in India Order) at http://dipp.nic.in/sites/default/files/publicProcurement_MakeinIndia_15June2017.pdf

[18] Draft National Policy on Software Products at http://meity.gov.in/sites/upload_files/dit/files/National%20Policy%20on%20Software%20Products.pdf

Public Procurement Preferences: Technology mandates and domestic preferences for government procurement have been clearly demonstrated as part of a larger "Make in India" initiative adopted by the Government of India.

The Make in India Order, issued by the DIPP in June 2017 to promote local manufacturing, requires every government department to give preference to local suppliers when procuring goods and services. Compared to previous legislation, the Make in India Order is the first enabling framework for preferential market access in software products and services. The order places an emphasis on the *situs* of manufacturing or provision of service (based on a definition of "local content"). However, government departments are granted the discretion to implement the Make in India Order according to their own requirements. The Ministry of Electronics and Information Technology (MEITY) is responsible for implementing the Draft Public Procurement (Preference to Make in India) Order 2017 – Notifying Cyber Security Products in furtherance of the Order (Draft Cybersecurity Products Notification), released in September 2017. [19]

The "local supplier" requirements under this Draft Cybersecurity Products Notification raise several challenges for BSA members. The requirements include mandatory incorporation and registration in India, ownership of IP rights by the Indian entity (use, distribution, and modification), domestic revenue accrual from exploitation of such rights, and ambiguity with respect to computation of value addition, among other implementation challenges. Moreover, the scope of products and services enumerated in the notification is extremely wide and may be subsequently revised to include other types of software products and services.

Such developments could significantly affect India's ability to acquire best-in-class products and services and negatively impact US companies' ability to effectively participate in public procurement exercises. In an effort to highlight these challenges and advocate for a fair and reasonable policy environment, BSA submitted written comments on the Draft Cybersecurity Products Notification and participated in stakeholder meetings organized by the government.[20] This Draft Notification was finalized by MeitY in July 2018 and released with minor changes.[21]

Data Localization: There are a variety of examples where the Government of India imposed, or proposes to impose, data localization requirements. In 2015, the Department of Electronics and Information Technology (the predecessor to MeitY) issued a request for proposals for provisional accreditation of cloud service providers (CSPs) which mandated "all services including data will have to reside in India."[22] In May 2017, MeitY released an open empanelment invitation for new cloud service offerings from CSPs, which also included a requirement for data localization of all eligible service providers.[23]

---

[19] Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products in furtherance of the Order at http://meity.gov.in/writereaddata/files/Draft%20Notficationn_Cyber%20Security_PPO%202017.pdf

[20] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/10262017BSACommentsonIndiaMEITyDraftCyberSecurityProductsNotification.pdf

[21] Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products at http://meity.gov.in/writereaddata/files/public_procurement-preference_to_make_in_india-order_2018_for_cyber_security_products.pdf

[22] Page 8 of 13 Guidelines for Government Departments On Contractual Terms Related to Cloud Services http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf (last accessed December 20, 2017)

[23] Page 33 of 73 Invitation for Application/Proposal for Empanelment of Cloud Service Offerings http://meity.gov.in/writereaddata/files/Application%20for%20Empanelment%20of%20CSPs.pdf (last accessed 4th January 2018)

India's Directive on Storage of Payment System Data (Directive) issued by the Reserve Bank of India (RBI) on April 06, 2018 without any advance public consultation, imposes data and infrastructure localization requirements — requiring payment systems operators "ensure that the entire data relating to payment systems operated by them (system providers) are stored in a system only in India."[24] Additionally, "data" is defined very broadly, and the Directive is likely to affect not only the payment processors, but also companies providing services to payment processors. BSA submitted comments to the RBI June 22, 2018, voicing concern about these data localization requirements.[25] The RBI provided payment firms a period of six months to comply with the Directive. This period elapsed on October 15, 2018 with the RBI refusing to extend the compliance deadline after repeated requests from industry. Although the RBI is not considering a suspension of services, it is exploring other actions it could take against non-compliant firms.

In the context of personal data protection, the Expert Committee provides justifications for the introduction of data localization requirements in chapter six of the Report issued to MeitY in July 2018, while also recognizing that data localization may impose a substantial economic burden on companies. The Personal Data Protection Bill, submitted to MeitY by the Expert Committee at the same time, also contains problematic data localization requirements.[26] The Bill requires that data fiduciaries store in India "at least one serving copy" of personal data subject to the Bill. BSA submitted formal comments on this measure in September 2018, exploring the challenges associated with data localization provisions in greater detail.[27]

As one more example of how the Government of India seems to be aggressively promoting the concept of data localization, MeitY established the Working Group on Cloud Computing (Working Group), under the chairmanship of Mr. Kris S Gopalakrishnan, co-founder of Infosys. It is reported that the recommendations of the Working Group include broad data localization requirements for both the public and private sector.

The US Government should use all available mechanisms, including formal bilateral dialogue, to urge the Government of India to carefully consider the narrow circumstances where it may be important for certain data to be maintained in India, and to refrain from imposing broad requirements that hinder innovation and digital trade without enhancing privacy or cybersecurity.

Cloud Computing: In June 2016, the Telecom Regulatory Authority of India (TRAI) released a consultation paper requesting stakeholder input on a range of important questions regarding cloud computing. In our submission to the TRAI, BSA noted that many of the issues raised in the consultation paper, such as interoperability and platform-to-platform migration, are best addressed by CSP-to-customer arrangements (such as contracts) rather than through a regulatory approach. Furthermore, BSA raised our concern that the TRAI or other government agencies in India might recommend data localization norms or impose India-unique standards or approaches to address the questions raised in the consultation paper.[28]

---

[24] Storage of Payment System Data: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0 last accessed: June 12, 2018

[25] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/06222018BSASubmissiontoReserveBankofIndia.pdf

[26] Personal Data Protection Bill (2018) at http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

[27] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/09282018BSACommentsonIndiaDataProtectionBill.pdf

[28] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/07252016BSASubmissiononCloudComputingIndia.pdf

The TRAI then released its recommendations in August 2017.[29] It is encouraging that the TRAI recommended a "light touch" approach to cloud computing regulation and emphasized the need for flexibility and choice by way of contractual agreements between CSPs and end-users. Unfortunately, it is unclear whether the TRAI is still considering potential server and data localization mandates.

The Department of Telecommunications released the National Digital Communications Policy – 2018 (NDCP 2018). Notably, the NDCP highlights its mission to make "India a global hub for cloud computing and data communication systems and services" by "enabling a light touch regulation for the proliferation of cloud-based systems."

The Working Group mentioned above is tasked with formulating a framework for promoting and enabling cloud services in India. It is also tasked with examining the cybersecurity and privacy aspects related to cloud computing.[30] The recommendations are expected to be published before December 2018.

Privacy and Data Protection: In July 2018, India issued the Personal Data Protection Bill prepared by the Expert Committee. Although many aspects of the Bill would lay a strong foundation for a robust personal data protection framework, several requirements pose substantial challenges to BSA members and other organizations that operate globally. In comments submitted September 28, 2018, BSA voiced its concerns and recommendations to MeitY.[31] As of October 2018, many other stakeholders have also provided their comments on the Bill, and MeitY is now examining the submissions with the aim of tabling a version of the Bill in the Winter Session of Parliament in December 2018.

BSA is largely concerned the Bill lacks the conceptual clarity and consistency that is crucial for the Indian digital economy to effectively integrate with the globalized data economy. Additionally, in terms of regulatory capacity, although the Bill establishes an independent regulator called the Data Protection Authority, BSA is concerned this regulating body would prove ineffective. These challenges, coupled with serious concerns about data localization, adequacy requirements, disproportionate criminal penalties, lack of flexibility for personal data fiduciaries, uncertain accountability requirements, lack of an institutional framework for enforcement, nonflexible security safeguards, improper liability allocation, and lack of harmonization pertaining to the personal data of children, are broken down in greater detail in our comments.[32]

In July 2018, a week before the Expert Committee published its Report and Draft Bill, the TRAI also submitted its recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector.[33] BSA had earlier submitted comments to the TRAI consultation process on privacy in October 2017 recommending that TRAI and other agencies of the Government of India work together and adopt clear and predictable stances on various issues relating to data protection.[34] While the future impact of TRAI's recommendations is unclear, TRAI's inputs will be relevant to the framing of the larger data protection framework in India, as they will remain a key participant in any related discussion.

---

[29] Telecom Regulatory Authority of India Recommendations On Cloud Services (2017) http://trai.gov.in/sites/default/files/Recommendations_cloud_computing_16082017.pdf

[30] Data Security Council of India Annual Report 2017-2018 at https://www.dsci.in/sites/default/files/documents/resource_centre/Annual-Report-2017-18.pdf

[31] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/09282018BSACommentsonIndiaDataProtectionBill.pdf

[32] Ibid.

[33] Recommendations On Privacy, Security and Ownership of the Data in the Telecom Sector (2018) at https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

[34]Comments available at https://www.bsa.org/~/media/Files/Policy/Data/10302017BSACommentsonIndiaTRAIConsultationonPrivacySecurityandOwnerhipoftheDataintheTelecomSector.PDF

Encryption: In September 2015, India published a Draft National Encryption Policy that was withdrawn shortly after publication. The draft raised a number of red flags, including restrictions on the use of commercially available encryption (e.g., by restricting key lengths) 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.

Intellectual Property

Patentability Guidelines for Computer-Related Inventions: Computer-Related Inventions (CRI) Guidelines issued in 2017 by the Controller General of Patents, Designs, and Trademarks (CGPDT) — the product of several years of deliberation, stakeholder engagement, and study — represent an improvement from previous versions and provide some finality to a long public discussion on this issue. Notably, the 2017 CRI Guidelines removed the "novel hardware" requirement for computer-related inventions. This is encouraging, as it is in line with international practice and recognizes the possibility of software-enabled inventions receiving patent protection in India. It will be important to monitor how the revised guidelines are applied in practice.

INDONESIA

Overview/Business Environment

The commercial environment for the software and IT sector in Indonesia is very challenging.[35] A variety of authorities have issued, or are in the process of developing, policies that will raise the cost of providing digital products or services to the Indonesian market.

Market Access

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.

Duties on Digital Products: In February 2018, the Ministry of Finance (MOF) issued Regulation 17, which amended Indonesia's Harmonized Tariff Schedule (HTS) to add Chapter 99 "[s]oftware and other digital products transmitted electronically." Although Chapter 99 is currently duty free, Chapter 99 effectively treats electronic transmissions as imports, to which customs requirements apply, including requirements to comply with all customs laws that attach to imports, prepare and file import declarations, and pay 10 percent value-added tax (VAT) and 2.5 percent income tax.

These compliance obligations are already burdensome for physical goods and require companies to have compliance departments composed of specialized trade professionals that can determine proper customs valuation, country of origin, HTS classification, and other requirements. Complying with Chapter 99 would not only prove very costly for companies, but in most cases these obligations simply cannot be applied to electronic transmissions.

Data Localization Requirements and Cross-Border Data Flows: The Government of Indonesia issued Government Regulation 82 on the Operation of Electronic System and Transaction (GR82) in October 2012. The Indonesian Ministry of Communication and Information Technology (MCIT) subsequently issued two implementing regulations under GR82: (1) Regulation No. 36 of 2014 on the Registration Procedure for Electronic System Operators; and (2) Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems (Electronic Data Protection Regulation). These regulations raise concerns regarding data and IT infrastructure 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 enhancing information security or protection.

More recently, on February 1, 2018, MCIT shared a Draft Amendment to amend GR82. BSA, along with several other trade associations, submitted comments to MCI, discussing the potentially problematic provisions within the text and calling for further clarification.[36] BSA's chief concerns focus on:

1. The wide scope of "electronic systems operator for public services";
2. The wide definition of "strategic electronic data"; and
3. Certain consequences of being deemed an "electronic systems operator for public services."

BSA recommends USTR works with the Government of Indonesia to ensure Indonesia's overall framework for information security and personal data protection will facilitate, rather than impede, the cross-border data transfers that are critical to growth and innovation in the global digital economy.

---

[35] *See generally*, BSA Cloud Scorecard – 2018 Indonesia Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Indonesia.pdf

[36] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/03012018BSAJointSubmissionOnGR82Amendment.pdf

Source Code Disclosure Requirement: MCIT is also considering two other GR82 implementing regulations on: (1) information security management; and (2) software used in electronic systems. If implemented, these regulations would require the disclosure of software source code by electronic system providers responsible for managing or operating computer systems used in connection with public services. BSA is deeply concerned about this requirement. Many global companies of leading-edge security technologies would withdraw from bidding opportunities that require them to turn over or disclose sensitive intellectual property, such as source code and other design information.

Over-the-Top Regulation: In mid-2016, MCIT published a draft regulation (which MCIT updated in mid-2017) on the Provision of Application and/or Content Services Through the Internet. This draft regulation threatens to impose unreasonable requirements on virtually all Internet-enabled services and service providers, including local physical presence and registration mandates, content filtering and censorship requirements, and mandatory use of local payment gateways, among others.

E-Commerce Regulation: In June 2016, the Government of Indonesia published a draft regulation on Electronic System Based Trade Transaction. This draft regulation threatens to impose unreasonable requirements on e-commerce providers relating to physical presence and registration, security clearance, infrastructure localization, and product liability, among other concerns. It also contains provisions on personal data protection that need to be aligned with the Draft Privacy Law and Electronic Data Protection Regulation discussed above.

The Draft E-Commerce Regulation has yet to be passed by the Government of Indonesia. This is despite the issuance by the Government of Indonesia of an E-Commerce Road Map 2017-2019 in 2017 (through Presidential Regulation 74 of 2017), indicating that the Draft E-Commerce Regulation should have been passed in October 2017.

REPUBLIC OF KOREA

Overview/Business Environment

The overall commercial environment in the Republic of Korea (Korea) for BSA members and the software sector is mixed.[37] Korea has a strong information technology (IT) market and a mature legal system. Over the past several years, however, the Government of Korea has adopted a number of policies that have erected substantial market access barriers to foreign software and IT products and services. Such policies include local testing requirements, and requirements to comply with national technical standards even when commonly used international standards are available. Although the Cloud Computing Promotion Act came into force on September 28, 2015, it remains difficult to provide cloud-based services to the Korean market. Data residency, physical network separation, and other requirements for sectors such as government/public services, finance, healthcare, and education hamper the ability to provide cloud-based services to users in these sectors.

The Government of Korea is actively developing its policies for moving Korea ahead in the digital economy. The Administration constituted a Presidential Fourth Industrial Revolution Committee in September 2017 to formulate and implement a strategic plan for this purpose. Government agencies have been reviewing regulations and considering regulatory reform or deregulation to stimulate innovation and growth in the digital economy. We urge the Government of Korea to use this opportunity to improve the overall business environment in Korea, especially for software and digital services.

Market Access

The adoption of procurement preferences for domestic firms and imposition of additional burdensome measures, often with security concerns cited as justification, have decreased market access for BSA members in Korea. These especially affect those providing Internet-enabled services, such as cloud-computing and data analytics services.

Cross-Border Data Flows and Server Localization: Although the Cloud Computing Promotion Act came into force on September 28, 2015, it remains a significant challenge for commercial cloud services providers (CSPs) who offer cloud services to public sector entities. This is due to the onerous certification requirements imposed by the Korea Internet Security Agency (KISA) on CSPs who provide cloud services to public sector agencies and the requirements for physical network separation. Similar guidelines and regulations requiring physical network separation or data on-shoring apply to the finance (see below) and healthcare sectors.[38] We remain concerned that, even after enactment of the Cloud Computing Promotion Act, significant barriers remain.

On August 29, 2018 the National Assembly passed a Bill amending the “Information and Communications Network Information Protection Act.” The Bill requires global companies without local presence in Korea to designate a representative with information protection duties in Korea and limits onward transfers of personal information to “third countries.”

Physical Network Separation: Although the Government of Korea is committed to promoting the adoption of cloud computing, security concerns by the National Intelligence Service (NIS) have resulted in policies requiring physical network separation, which prevent or discourage government agencies and other regulated sectors (e.g., finance and healthcare) from adopting commercial cloud computing and related services.

---

[37] *See generally*, BSA Cloud Scorecard – 2018 Korea Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Korea.pdf

[38] E.g., under the Medical Services Act.

The Regulation on Supervision of Electronic Financial Transactions (RSEFT) was amended on October 5, 2016 to permit the use of cloud services by financial services institutions (FSIs), by allowing certain data to be stored on public cloud services. However, this amendment only expanded the ability to store non-critical information on the cloud. FSIs still cannot use cloud computing services to process "important" information — including personal data, such as the financial data of individuals, which comprises the bulk of the data FSIs handle — as this data remains subject to data localization and physical network separation requirements.[39]

Personal Information Protection Regime: Korea's personal information protection (PIP) regime is one of the most stringent in the region and has significantly decreased the ability for BSA members to serve the Korean market. The two relevant pieces of legislation — the Personal Information Protection Act and the Act on Promotion of Information and Communication Network Utilization and Information Protection — impose onerous and prescriptive obligations, many of which restrict cross-border transfers of personal information that are necessary for overseas-based service providers to serve the Korean market.

Regulators are currently reviewing and looking to streamline Korea's PIP regime, partly due to Korea joining the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) System. This presents a good opportunity for Korea to recalibrate its regime and adopt measures that allow for more flexible data handling by businesses, which is critical to investment and innovation in emerging technologies like data analytics and machine learning, while ensuring that personal information is appropriately and adequately protected.

Discriminatory Security Certification Requirements Applied for Foreign IT Products: Since 2011, the Government of Korea has imposed additional security verification requirements for international Common Criteria-certified information security products that are procured by government agencies. However, no such requirement is applied to locally certified products. In 2014, the Government of Korea extended similar security conformity testing requirements to international Common Criteria-certified networking products procured by any Korean government agency.

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 Common Criteria-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, a separate conformity test is required for each government agency, even for products procured and verified by another government agency.

While the Government of Korea has indicated that it intends to change the policy, it has yet to issue any formal correction in writing. It therefore remains unclear what the applicable requirements are.

[39] E.g., under the Financial Services Commission's (FSC's) Regulation on the Supervision of Electronic Financial Activities there is a physical network separation requirement for information processing systems used by financial services institutions. The FSC relaxed this requirement in 2016 for "non-critical" information processing systems so that while network separation is still required for such systems, this requirement can now be met through logical/virtual separation instead of physical separation. Physical network separation is still required by the regulation for "critical" information processing systems and this significantly limits the use of cloud computing in the financial services sector.

THAILAND

Overview/Business Environment

The Royal Thai Government (RTG) is pursuing a range of policies under Thailand 4.0 to promote the digital economy. Two important pieces of legislation under consideration — one on cybersecurity protection of critical infrastructure, and the other on personal data protection — are important elements of this effort. BSA agrees that it is important for Thailand to enact robust and effective cybersecurity and personal data protection legislation. However, we remain concerned that both bills, as currently drafted, could undermine the RTGs efforts to enhance cybersecurity and personal data protection, interfere with the government's broader goals to drive Thailand 4.0, and unfairly impede BSA member companies' ability to effectively provide products and services to the Thai market.[40]

Market Access

BSA shares the goals of the RTG's Digital Economy initiative, Thailand 4.0, and supports the thoughtful enactment of necessary legislation regarding privacy and cybersecurity. Before finalizing such legislation, however, the RTG should minimize unintended effects that will harm the ability of BSA members and other technology sector companies to provide innovative and effective software products and services.

Security: Thailand's 2015 National Cybersecurity Bill was designed to strengthen the cybersecurity capabilities of government agencies and provide appropriate breach notification procedures. However, the bill raised concerns because it gave the Office of the National Cybersecurity Committee (ONCC) broad powers to access confidential and sensitive information without sufficient protections to appeal or limit such access. In our 2015 comments, BSA highlighted that granting the ONCC such broad powers would undermine public confidence and trust in information technology (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.[41]

In April and May 2018, BSA (along with the US-ASEAN Business Council) submitted comments to Thailand's Ministry of Digital Economy and Society (MDES) on the 2018 version of the National Cybersecurity Bill.[42] BSA's chief concerns center around: the composition of the National Cybersecurity Committee, the broad powers of the NCSC, the notification regime for cyber-attacks, surveillance authority, and criminal liability.

MDES released another, purportedly near final, version of the National Cybersecurity Bill in September 2018, upon which BSA filed another set of comments, focusing on similar concerns that we have described in the past.[43]

---

[40] *See generally*, BSA Cloud Scorecard – 2018 Korea Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Korea.pdf

[41] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/05062015SubmissionCybersecurityBill_EN_DeputyPrimer.pdf

[42] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/05212018enJointBSA_USABC_SupplementalCommentsThaiCybersecurityBill.pdf

[43] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/10122018EN_BSACommentsCybersecurityBillwith%20Annexes.pdf

As of October 2018, we understand that the National Cybersecurity Bill has been returned to the Council of State for further consideration before it will be introduced to the Cabinet and the National Legislative Assembly (NLA), respectively.

Privacy: The Personal Data Protection Bill (PDP Bill) is also under review by the Council of State. It is designed to build public trust and confidence in the digital economy and to implement the Asia-Pacific Economic Cooperation (APEC) Privacy Framework's principles for cross-border data transfers. The most recent version also heavily draws from the recently implemented General Data Protection Regulation (GDPR) of the European Union.

Since 2015 when we first submitted comments on Thailand's PDP Bill, BSA has highlighted the importance of protecting personal information to foster the trust and confidence necessary for growth of the digital economy.[44]

In our most recent comments to MDES on the January 2018 version of the PDP Bill, BSA noted the significant improvements over earlier drafts and proposed recommendations on several provisions that still threaten to create unreasonable burdens and legal uncertainty for the technology sector.[45] BSA's chief concerns surround unclear or unreasonable obligations on personal data processors, the still too limited legal bases for handling personal data, potential impediments to international data transfers, certain elements of data breach notification system, and the scope and limits of the powers of the Personal Data Protection Committee (PDPC) and Expert Committees.

In September 2018, the Council of State issued another version of the PDP Bill. This new draft introduced new provisions, apparently drawn from the GDPR. While introducing the additional consumer rights that exist in the GDPR is a positive step, our preliminary analysis indicates that the drafters failed to bring in the flexibilities for processing, handling, and transferring data that exist in the GDPR. Furthermore, the concerns and recommendations we made in our February 2018 comments remain unaddressed.

[44] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/03232015BSASubmissiononThaiPersonalDataProtectionAct_EN.PDF

[45] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/02062018BSASubmissionThaiPersonalDataProtectionBill.pdf

VIETNAM

Overview/Business Environment

Over the past several years, Vietnam has enacted, implemented, and proposed measures to regulate the software sector, which are likely to reduce fair and equitable market access for BSA members wishing to provide software products and online services in Vietnam.[46] The enactment of the Cybersecurity Law in in June 2018 and current efforts to develop implementing rules only exacerbate the problems and threaten to make Vietnam an even less attractive destination for the delivery of cutting-edge software products and services.

Market Access

Cybersecurity: On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the 20th version of the Cybersecurity Law (Law). Currently, we understand the Ministry of Public Security (MPS) is developing implementing measures with the aim of issuing final rules before the Law goes into effect January 1, 2019.

The Law raises a number of serious concerns and will likely significantly impact the ability of many BSA members to provide software products and services in Vietnam. Specifically, the law requires data to be stored in Vietnam, requires all service providers to have a local presence in Vietnam, and grants authorities the ability to restrict international data transfers and require the disclosure of content in unencrypted form. The breadth of the Law far exceeds cybersecurity protection and extends to a broad regulation of the Internet generally. This coupled with the vast powers granted to authorities, and stringent requirements, such as requiring software product and service providers to comply with local cybersecurity standards and regulations and to apply for certification by local agencies, is a significantly negative development in Vietnam's market access environment for the software sector.

BSA urges USTR to work with the Government of Vietnam to ensure that the implementation of the Law is managed in a way that minimizes unnecessary costs and disruptions to BSA members while enhancing the government's legitimate objectives of enhancing cybersecurity capabilities in Vietnam.

Information Security: The National Assembly enacted the Law on Network Information Security (LONIS) on November 19, 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 entering the market, overly broad definitions of personal information, and overly broad provisions requiring "cooperation with the Government" regarding access to data, which include requirements to decrypt encrypted information held by third parties. These provisions impact the ability of BSA members to provide services in Vietnam. It also is unclear how the LONIS and the Cybersecurity Law will interact, raising additional uncertainty and compliance costs for BSA members.

Cross-Border Data Flows and Server Localization: On September 1, 2013, Decree No. 72 went into effect.[47] The decree imposes onerous server localization requirements and restrictions on cross-border data flows that will undermine the ability of BSA members to provide digital services. In early 2015, the Government of Vietnam proposed further elaborations on these requirements in a Draft Circular. The Draft Circular also requires 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.

---

[46] *See generally*, BSA Cloud Scorecard – 2018 Vietnam Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Vietnam.pdf

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

EUROPEAN UNION

Overview/Business Environment

American data service providers are confronting growing challenges to providing innovative digital services in Europe. European authorities, both at the state level and at the European Union (EU), are considering and adopting measures that represent *de facto* market access barriers. Several of these measures may significantly restrict data flows. While BSA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, these policies would block US firms from offering digital services in the EU. Moreover, there are legal challenges underway that could invalidate important existing mechanisms for transatlantic data transfers, such as the US-EU Privacy Shield and standard contractual clauses, adding further uncertainty for US data services providers.

Market Access

The number of current or proposed policies that act as barriers to data services and digital trade are increasing in the EU and are of major concern to BSA members. BSA asks that the US Government closely follow these developments in Europe, work intensively to protect existing transatlantic data transfer mechanisms, and push back against policies that pose the most significant market access barriers.

Data Flows: Measures that impede the flow of data across borders impose substantial burdens on US service providers and negatively impact US jobs. European authorities are focused on data transfers to the United States and have not applied the same scrutiny to data transfers to any other market 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 transfers 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). While Digital Rights Ireland's challenge has been dismissed, the General Court is looking at the merits of the second challenge. These groups contend that US practices on law enforcement and national security access to data lack sufficient privacy safeguards, and as such, the Privacy Shield should be invalidated. These legal challenges mean US companies will face continuing uncertainty in relying on the Privacy Shield for transatlantic data transfers.

In May 2016, the Irish Data Protection Commissioner requested that the Irish High Court ask the Court of Justice of the European Union ("CJEU") to examine whether Standard Contractual Clauses ("SCCs") violate EU citizens' fundamental rights insofar as there is insufficient judicial redress for EU citizens when their data is transferred to third countries, such as the US. In May 2018, the Irish High Court finalized its Order for Reference to the CJEU, including 11 questions on the legality of the SCCs, the adequacy of the US legal system, and the legality of the Privacy Shield. In July 2018, the case and questions from the Irish High Court were docked at the CJEU and BSA was officially accepted as amicus curiae at the CJEU.

Data Flows in Trade Agreements with Third Countries: In February 2018, the European Commission released a draft text on data flows in trade agreements, seeking to address concerns from Member States, trading partners, and industry that EU free trade agreements ("FTAs") suffer from a lack of language on the free flow of data. The European Commission aims to insert the draft text into future FTAs as a way to stop third countries from restricting the flow of data through localization requirements, with the stated intention of ensuring that the EU's data protection rules are not weakened. Despite the positive intentions of the European Commission, the data flows text would actually undermine the flow of data between trading partners due to broadly constructed, self-judging exceptions. In mid-2018, the European Commission decided to move ahead with this draft language despite initial concerns from Member States and the European Parliament regarding its potential negative impact on data flows. In May 2018, the EU began FTA negotiations with Australia and New Zealand, in which it is intent on including this data flows language.

Dual-Use Export Controls Regulation: In September 2016, the European Commission published a Regulation aimed at revising the EU's regime for the control of exports and dual-use items. The draft legislation represents a deviation from the current international controls regime and could lead to tighter export controls, increased administrative burdens, and a potential risk for exporters of cybersecurity software products and services.

Proposed e-Privacy Regulation: In January 2017, the European Commission published a Regulation aiming to update the EU's current e-Privacy Regulation (ePR), which regulates the confidentiality of communications and processing of personal data on terminal equipment. The scope of the proposed regulation is very broad, sweeping in any electronic communications service provided with the use of a public communications network, including over-the-top services and machine-to-machine communications (e.g., data transfers between Internet of Things devices). It also would apply extraterritorially, including in circumstances where processing is conducted outside the EU in connection with services provided within the EU. The draft Regulation built around a consent-only processing model, risks contradicting key provisions of the General Data Protection Regulation ("GDPR"). BSA submitted comments, expressing concern for the wide-reaching and prescriptive rules included in the ePR and the narrow number of exceptions.[48]

In October 2017, the European Parliament adopted its position on the draft Regulation. The Council has yet to adopt a negotiating position on the draft legislation, with numerous Member States expressing continued concern over the impact of the new law on the EU's digital economy.

EU Cybersecurity Competence Centre: In September 2018, the European Commission published a draft Regulation on the establishment of the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The European Commission's proposal seeks to create an EU Cybersecurity Competence Centre aiming to ensure that Europe retains and develops essential cybersecurity technological capacities to protect critical networks and information systems, provides key cybersecurity services, and competes more effectively on the global cybersecurity market. If adopted as proposed, there is a risk that research funding and procurement decisions of the proposed Competence Centre may disadvantage some US-based companies, particularly in relation to: (i) provisions governing funding and procurement; and (ii) industry's involvement in the work of the proposed Competence Centre.

Intellectual Property

Text Data and Mining: In September 2016, the European Commission proposed new copyright rules which create a specific, but narrow exception to perform text and data mining ("TDM") for non-public interest research organizations. In May 2018, the Council reached its position on the draft Directive. The European Parliament is in the process of adopting its position on the proposed Copyright Directive. In July 2018, the European Parliament rejected the initial report on the draft Directive. In September 2018, the European Parliament endorsed the JURI Committee draft Report, and on October 2, the "trilogues" between the European Commission, European Parliament, and Council started, with the aim to finalize discussions prior to the 2019 European elections. The final text is expected to allow Member States to enact an optional national exception for all actors engaging in reproductions and extractions of lawfully accessible works that form part of the process of TDM. To the extent that certain Member States do not implement such a national exception, the ability of BSA members to perform TDM may be undermined, resulting in barriers to digital trade in those countries.

[48] Comments available at https://www.bsa.org/~/media/Files/Policy/Data/09202017BSAPositionPaperontheEUePrivacyRegulation.pdf

BRAZIL

Overview/Business Environment

Brazil is seeking to create an environment that leverages emerging technologies, including artificial intelligence. Brazil has demonstrated a certain willingness to engage in more open dialogue with stakeholders, which resulted in some positive policy developments, but the overall market environment in Brazil remains challenging. A variety of existing and proposed measures related to cybersecurity (tied to public procurement), privacy, and domestic procurement preferences have created, or threaten to create, *de facto* market access barriers for BSA members. Discussion and implementation of relevant policies may also be delayed as a result of the new Administration assuming office in early 2019.

Market Access

Privacy Legislation*:* After more than four years of discussion, the Brazilian Congress approved the Data Privacy Bill in July 2018. The Bill was signed into law by the Brazilian President in August 2018, but some provisions were vetoed, including those that created the Data Protection Authority (DPA). The Brazilian Congress is scheduled to analyze the vetoes by the end of 2018, and it is not expected to oppose them. Regulatory efforts to create a DPA are ongoing and should be finalized in 2019. Ensuring proper implementation of the law will be key to avoid adverse impact on US companies operating in the Brazilian market.

Data and Server Localization Requirements: The Guidelines on Government Procurement of Cloud Services were issued in draft format in 2017 and are currently pending. If finalized and implemented as drafted, the guidelines will create server and data localization requirements that will negatively impact procurement of cloud computing services by all Federal agencies. BSA submitted comments on the draft guidelines urging the Government of Brazil to remove the localization requirements but, unfortunately, there are no indications that the regulation will be modified to address the issue.[49] BSA urges the US government to establish a dialogue with the new Administration to demonstrate the importance of the elimination of data localization requirements.

Government Procurement Barriers*:* Presidential Decree 8135/2013 (Decree 8135) regulates the use of IT services provided to the Federal government by private 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 serious challenges for BSA members, especially the deviation from global standards and requirements to disclose source code and other IP. In 2016, the Federal government announced it would revoke Decree 8135. A new decree was expected to be published by the end of 2016, but the new decree is still pending to this date. The new decree and implementing regulations should allow Federal agencies to procure innovative IT products and services, including cloud computing, and avoid restrictive data localization policies.

Government Procurement Preferences*:* Presidential Decree 8186/2014 establishes an 18 percent price preference for the following categories: software licenses, software application development services (customized and un-customized), and maintenance contracts for applications and programs.
Public procurement preference for local products and services, as well as technologies developed in Brazil, would also be required by the pending Guidelines on Government Procurement of Cloud Services, which was published in draft format in early 2017 (Please see Data and Server Localization item above). In addition, the Brazilian Congress is currently discussing potential changes to Brazil's Procurement Law. According to current law, the public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of IT systems can only be limited to local goods and

[49] Comments available at https://www.bsa.org/~/media/Files/Policy/Filings/CommentsBSA_CloudProcurement.pdf

services if 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. Although efforts to approve the bill are currently stalled, should the bill be approved in the future, 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.