October 31, 2019

Docket No. USTR-2019-0012

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 (84 Fed. Reg. 46079, September 3, 2019) 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 National Trade Estimate on Foreign Trade Barriers (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, data analytics, machine learning, cybersecurity solutions, and more. The software industry is responsible for $1.6 trillion of total US value added GDP. The industry supported 3.1 million jobs (directly) and 14.4 million jobs (indirectly) — jobs that pay more than twice the national average for all occupations.[2] BSA members are among the top US patent recipients (accounting for nearly 80 percent of all US patents issued to US companies among the top 10 patent grantees)[3] and annual US software research and development (R&D) investments totals US$83 billion.

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

[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, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] Software.org, Growing US Jobs and the GDP (Sept. 2019), available at: software.org/wp-content/uploads/2019SoftwareJobs.pdf

[3] IFI Claims Patent Services, 2018 Top 50 US Patent Assignees (accessed Oct. 1, 2019) ("2018 Top 50 US Patent Assignees"), available at: https://www.ificlaims.com/rankings-top-50-2018.htm. BSA members accounted for 16,348 of the 20,771 patents issued to US companies within the top 10 patent recipients in 2018).

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.

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 addresses three major issues: Trade Barriers, Innovation, and Privacy and Security..[4] In each of these areas, it is critical for policymakers to be vigilant against the creation

[4] BSA's Digital Trade Agenda is available at https://www.bsa.org/files/policy-filings/05072019bsa_advancingdigitaltradeagenda.pdf. The three major section of the Digital Trade Agenda address the following: (1) Trade Barriers - data localization requirements, cross-border data transfer restrictions, customs requirements on electronic transmissions, mandatory national standards, forced technology transfer requirements,

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.

In the 2018 Global Cloud Computing Scorecard (Cloud Scorecard) BSA ranked countries' preparedness for the adoption and growth of digital services, assessing each country's legal framework relating to IP, trade, privacy, and cybersecurity, among other areas.[5] While Germany, Japan, Singapore, the United Kingdom, and the United States score well in this report, especially in relation to IP and trade, China, India, Indonesia, Russia, and Vietnam do not. BSA members face significant challenges in these latter markets.

In this submission, BSA discusses trade barriers in the following markets: Brazil, China, India, Indonesia, South Korea, Thailand, Vietnam, and the European Union (EU).

Market Access and Intellectual Property Issues in Select Economies

To realize the economic promise of software, cloud computing, and emerging technologies, it is important to establish a legal framework that fosters innovation and promotes confidence in the digital economy. BSA's Cloud Scorecard examines the critical factors of such a legal framework, including in relation to international trade, privacy, cybersecurity, IP, voluntary standard-setting, and information technology (IT) readiness. Japan, Singapore, and the United States score well in this report due to their forward-looking trade, IP, and innovation policies (including their support for rules to permit data analytics). In contrast, China, India, Indonesia, Russia, and Vietnam receive the lowest rankings of all countries reviewed, due to policies that undermine not only investment in software innovation, but also market access for US IPR holders.
We highlight key market access and intellectual property issues below, exploring: (1) cross-border data flows and data localization; (2) security; (3) standards; (4) customs requirements on electronic transmissions; (5) artificial intelligence and machine learning; (6) Internet Service Provider (ISP) liability and safe harbors; (7) patents; (8) trade secrets and other proprietary information; (9) software license compliance; (10) government and state-owned enterprise (SOE) legalization; and (11) procurement restrictions.

Cross-Border Data Flows and Data Localization: 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. 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 policy means chosen are often significantly more trade-restrictive than necessary to achieve any legitimate public policy goal. Immediate attention to these threats is urgently needed. Unfortunately, some markets, including **China, India, Indonesia, Nigeria, and Vietnam**, have adopted or have proposed rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory.

Among several Chinese measures that restrict the ability to transfer data across borders, the draft 2017 Critical Information Infrastructure Protection regulations would effectively require all cloud computing services providers (CSPs) to store data in-country.[6] India too has imposed data localization requirements, including through India's Directive on Storage of Payment System Data issued by the Reserve Bank of

---

preferential treatment for state-owned enterprises, investment and export restrictions, procurement restrictions, and restrictions on choice of software and technology products; (2) Privacy and Security – protecting privacy and security, encryption, protecting the IT supply chain, and promoting fair and transparent requests for access to data; and (3) Innovation – machine learning and data analytics, open government data, appropriate limitations on liability relating to third party conducts, copyright, patents and trade secrets, R&D, innovative technology in government, and electronic signatures.

[5] BSA's 2018 Global Cloud Computing Scorecard at:
https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf

[6] *Critical Information Infrastructure Protection Regulations (Draft for Comment)*, July 11, 2017 (Chinese) at:
http://www.cac.gov.cn/2017-07/11/c_1121294220.htm

India in 2018, which imposes data and infrastructure localization requirements.[7] Likewise, Vietnam's 2018 Cybersecurity Law[8] and draft implementing regulations impose improper data localization requirements. Similarly, Nigeria's Guidelines for Nigerian Content Development in Information and Communications Technology contain stringent local content and sourcing requirements that apply to both government and private sector purchases. These guidelines raise significant market access concerns for companies offering software, information technology (IT), and data services overseas.

BSA also continues to monitor the application of measures in the **EU** that govern cross-border data flows, as well as EU's bilateral and plurilateral trade negotiations and developing legal jurisprudence which could dramatically restrict cross-border data flows with Third Countries.

Measures that impede cross-border data flows and mandate data localization requirements are gravely disruptive to international trade. BSA urges the United States to work with its trading partners to prevent or remove such practices.

Security: Governments have a legitimate interest in ensuring software products, services, and equipment deployed in their countries are reliable, safe, and secure. However, some markets — including **Brazil, China, India, Korea, Thailand, and Vietnam** — are using or proposing to use security concerns to justify *de facto* trade barriers. Requiring cloud service providers to confine data in-country does not improve security, but ultimately hinders it — preventing data from being backed up in multiple locations. Ultimately, 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 software-enabled services and 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, some countries have developed or are developing country-specific standards to favor local companies and protect them against foreign competition. This creates *de facto* trade barriers for BSA members, raises the costs of cutting-edge technologies for 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**.

Customs Requirements on Electronic Transmissions: Across a broad cross-section of economic sectors, there are growing concerns about proposed domestic policies to improperly impose customs requirements on US digital exports — a development that would directly impact the United States' most innovative industries, including software and cloud computing services. Since 1998, World Trade Organization (WTO) Members have maintained a moratorium on customs duties on electronic transmissions. However, in 2018 **Indonesia** issued Regulation No.17/PMK.010/2018 (Regulation 17), which amends Indonesia's Harmonized Tariff Schedule to add Chapter 99: "[s]oftware and other digital products transmitted electronically."[9] These new tariff lines would cover many US digital exports — potentially everything from subscription services for music, film, and publications; to cloud and other remote software services; to data used in manufacturing plants; and a broad catch-all category of "other digital products." Other countries appear to be following Indonesia's path. India and South Africa are working to undermine support for the WTO e-commerce moratorium[10] and push a work program at the World Customs

[7] *Reserve Bank of India Storage of Payment System Data Directive (2018)* at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0

[8] *Vietnam's 2018 Cybersecurity Law* at: https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-luat-an-ninh-mang-so-24-2018-qh14-164904-d1.html#noidung

[9] Regulation 17 purports to cover a wide array of categories, classified in Indonesia's tariff schedule between subheadings 9901.10.00 to subheading 9901.90.00, including "multimedia (audio, video or audiovisual)"; operating system software; application software; "support or driver data, including design for machinery system"; and a broad catch-all category covering "other software and digital products."

[10] WTO submission by India and South Africa, "Moratorium on Customs Duties on Electronic Transmissions: Need For A Re-think ," July 12, 2018: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-

Organization to impose customs requirements on electronic transmissions. If successful, these misguided efforts threaten to increase costs of digital products and services, and reduce productivity across sectors, in economies that would otherwise benefit from BSA members' software and technologies.[11]

Artificial Intelligence and Machine Learning: Appropriate legal frameworks are critical to data-enabled innovations, including artificial intelligence (AI), machine learning, cloud-based analytics, and the Internet of Things (IoT). AI, machine-learning, and analytics systems are "trained" by ingesting large data sets to identify underlying patterns, relationships, and trends that are then transformed into mathematical models that can make predictions based on new data inputs. Following US leadership in this area, trading partners in East Asia, Southeast Asia, and Europe are taking a range of approaches to modernize their legal frameworks to permit the future development of, and international competition in, AI systems.

First, Japan enacted the Copyright Law Amendment Act ("the Act") in May 2018, which helps innovative US companies compete effectively in the Japanese market. Importantly, Article 30-4 of the Act permits both commercial and academic institutions to engage in data analytics, including through the creation of machine-readable copies that can be digitally analyzed and maintained for data validation purposes, provided that the user has lawful access to the data. Second, in January 2019, Singapore issued its Copyright Review Report, setting out its decision to amend the Copyright Act to (among other things) include a carefully calibrated framework permitting data analytics to be performed for both non-commercial and commercial purposes (subject to requirements of lawful access – e.g. via a paid subscription).[12] Third, in the EU, similar legislation was also passed, with copyright exceptions for both academic and commercial institutions – while preserving the right for rightsholders to reserve against "text and data mining." Finally, in the United States, the "non-consumptive" reproductions that are necessary for the development of AI-related technologies are considered fair use. Thus, across four major legal systems, an emerging international legal consensus provides the business certainty necessary for the development of new AI-related products and services. BSA urges the US government to continue promoting such AI-focused legal frameworks — not only to foster innovation and creativity, but as a means of maintaining US technology leadership in AI and opening foreign markets to innovative US companies.[13]

Copyrights: Innovation in the digital environment requires legal frameworks that provide copyright holders with the tools necessary to effectively enforce their copyrights. An effective framework for online copyright enforcement must balance the legitimate needs and interests of all parties with a role in driving innovation, including content creators, ISPs, online platform providers (i.e., intermediaries), and members of the public. These interests are best accommodated through safe harbor frameworks that provide online intermediaries with limitations on monetary liability for third party content in exchange for removing content upon notification of claimed copyright infringement from a relevant rights holder. Although a statutory safe harbor framework is a well-established international best practice reflected in the US and Singaporean legal systems (among others), other countries have yet to modernize their copyright frameworks in this regard.

DP.aspx?language=E&CatalogueIdList=247027,247023,246849,246824,246785,246786,246779,246780,246766,246733&CurrentCatalogueIdIndex=8&FullTextHash=

[11] Indonesia and India have also imposed tariffs on Information and Communications Technology (ICT)-related products that are at odds with their WTO commitments. In Indonesia, these tariffs are being applied under HS subheadings 8517.62.49 and 8517.62.10, and in India under various headings, including under HS 7017, 7920, 8486, 8504, 8517, 8518, 8525, 8529, 8542, 8544, 9030, 9031. This creates significant uncertainly for BSA members importing products into these countries.

[12] Singapore Ministry of Law, Singapore Copyright Review Report, pp. 32-34 (Jan. 17, 2019), available at: https://www.mlaw.gov.sg/content/dam/minlaw/corp/News/Press%20Release/Singapore%20Copyright%20Review%20Report%202019/Annex%20A%20-%20Copyright%20Review%20Report%2016%20Jan%202019.pdf

[13] See *BSA | The Software Alliance, Comments on the Draft 2018-2022 Strategic Plan of the United States Patent and Trademark Office* (September 18, 2018), pp. 4-5, available at: www.bsa.org/~/media/Files/Policy/IntellectualProperty/09202018USPTOCommentsonDraft20182022StrategicPlan.pdf

Patents: BSA members invest enormous resources to develop cutting-edge technologies and software-enabled solutions for businesses, governments, and consumers.[14] It is 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.

Trade Secrets and Other Proprietary Information: BSA members 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 to protect 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 challenges not only in the country in question, but also globally. Countries with weak trade secret protection rules, or that have (or are proposing) policies requiring disclosure of sensitive information include **China, India, and Indonesia.** In addition, countries including **China and Indonesia** have implemented or proposed policies, such as sector-specific outsourcing or IT risk management frameworks, that require source code review of technologies or services.

Procurement Restrictions: Governments are among the biggest consumers of software products and services, yet many impose 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.**

Conclusion

BSA welcomes the opportunity to provide this submission to inform the development of the 2020 National Trade Estimate and the United States' engagement with important trading partners in 2020. 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.

[14] 2018 Top 50 US Patent Assignees, *op. cit.* BSA members represented four of the top 10 US patent recipients in 2018, accounting for 47 percent of all US patents issued in 2018 to the top 10 recipients.

Table of Contents

BRAZIL

Overview/Business Environment

Since President Bolsonaro took office in January 2019, the Brazilian and US governments have engaged in positive dialogues in various areas. For example, recent positive policy developments include the revocation of a decree that contained troublesome software auditing and source code disclosure requirements in the context of public procurement. Brazil's recently issued guidelines on IoT are also positive, although they have a broad scope of application. The Government of Brazil is seeking to increase the use of digital tools by federal agencies, and to create an environment that leverages emerging technologies, including artificial intelligence.

Even though Brazil has taken positive steps to improve market access recently, the overall market environment in Brazil remains challenging. Current and pending legislation in the areas of privacy, public procurement of cloud services, as well as domestic procurement preferences have created, or threaten to create, *de facto* market access barriers for BSA members.

We urge the US government to leverage the positive dialogues it has advanced with Brazil, including potential trade discussions to promote the elimination of current market barriers that impact US companies' ability to do business in Brazil.

Market Access

***Privacy Legislation**:*

The Brazilian Congress approved the Brazilian Personal Data Protection Bill in August 2018, and the law will come into force in August 2020. Legislation authorizing the creation of the Data Protection Agency (DPA) was approved in July 2019, but the DPA has yet to be fully established. DPA leadership appointments, other staffing decisions, as well as budget allocations are currently pending. The lack of a strong and properly funded DPA would have negative effects on the implementation of the Personal Data Protection Law and would impair cross-border data flows that are critical to market access for US companies selling goods and services in Brazil.

Data and Server Localization Requirements: The Guidelines on Government Procurement of Cloud Services were issued in late 2018, and include 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 Brazil to remove the localization requirements. However, Brazil did not adopt these recommendations, and the final Guidelines include the localization requirements. .[15]

***Government Procurement Preferences**:* Presidential Decree 8186/2014 establishes an 18 percent price preference for local products and guidelines for the following categories: software licenses, software application development services (customized and un-customized), and maintenance contracts for applications and programs. Public procurement preferences for local products and services, as well as technologies developed in Brazil, are also required by the Guidelines on Government Procurement of Cloud Services issued in 2018. ,

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 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.

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

CHINA

Overview/Business Environment

BSA members and other international technology providers face a particularly challenging commercial environment in China — especially from a market access perspective.[16] BSA members recognize the importance of resolving longstanding bilateral challenges with China and have seen first-hand the challenges and evolution of China's policies in the technology sector. BSA supports continued dialogue by the US and Chinese governments to work towards achieving mutually beneficial solutions to these challenges.

To elaborate on how China continues to present major challenges to BSA members in terms of market access, in 2017 and 2018, the Government of China issued numerous policies and standards designed to implement the Cybersecurity Law.[17] The law raises significant market access challenges relating to data localization, security, and privacy, which could be exacerbated or mitigated depending on how its 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 vague requirements and is frequently interpreted by regulated entities as an instruction from the government to procure only domestic products and services.

Beyond cybersecurity, China's regulatory regime also makes it extremely difficult for BSA members to participate in the digital market. The existing system 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. In December 2018, China unveiled the latest draft of the proposed Foreign Investment Law, which contains commitments that appear to assure foreign investors of a more level playing field and better protections for investments (e.g. against state expropriation) and intellectual property (IP).[18] However, it remains unclear how the draft Foreign Investment Law will be implemented, if adopted, and if the challenges and concerns raised in this submission will be addressed. BSA urges the United States to continue to engage closely 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

[16] 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

[17] *Cybersecurity Law of the People's Republic of China*, November 11, 2016 (CSL) (Chinese) at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm. Unofficial English translation at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[18] *Foreign Investment Law of the People's Republic of China (Draft)*, December 26, 2018 (Draft Foreign Investment Law) (China), at: http://www.npc.gov.cn/npc/flcazqyj/2018-12/26/content_2068280.htm. The Draft Foreign Investment Law will, if adopted, replace 3 existing laws in China relating to foreign investments — the Law on Chinese-Foreign Equity Joint Ventures, the Law on Contractual Joint Ventures, and the Law on Wholly Foreign-Owned Enterprises.

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.[19] 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 CSL. 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 (e.g., requiring that all personal information and important information collected in China, and not just by CII operators, must be held in-country).

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 is the Internet Security Supervision and Inspection Provisions by Public Security Organs released by the Ministry of Public Security (MPS) in September 2018, which codified and conferred broad authorizations for public security bodies to enforce the CSL.[20] This includes, among other things, the ability for public security bodies to conduct on-site and remote cybersecurity inspections on a broad (and indeterminate) range of companies that process and redistribute data or provide Internet services, and to impose a range of penalties (including fines and detention of individuals) for non-compliance.

Cybersecurity Classified Protection Regulation: On June 27, 2018, China established a de facto cybersecurity protection baseline for network operators and a universal compliance framework for the CSL by releasing the draft Cybersecurity Classified Protection Regulations (CCPR)[21] — 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.[22] Like MLPS, CCPR 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.

The draft CCPR also imposes several significant requirements regarding the structure and maintenance of networks operating within China. For instance, the draft CCPR requires that systems at Level 3 and above be connected with China's Public Security Bureau (PSB) system (managed by MPS) and that technical maintenance for such systems be performed within China. These unnecessarily intrusive requirements threaten to shut foreign technology out of systems ranked at CCPR 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 replace all international algorithms and schemes with those developed domestically. Such changes to algorithms or encryption mechanisms create technical barriers to trade and undermine interoperability.

---

[19] CSL, *op.cit.*

[20] *Internet Security Supervision and Inspection Provisions by Public Security Organs*, September 15, 2018 (Chinese), at: http://www.mps.gov.cn/n2254314/n2254409/n4904353/c6263180/content.html

[21] *Cybersecurity Classified Protection Regulations (Draft for Comment)*, June 27, 2018 (CCPS) (Chinese), at: http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html?from=timeline&isappinstalled=0

[22] *Administrative Measures for the Multi-level Protection Scheme of Information Security*, June 22, 2007 (MLPS) (Chinese), at: http://www.mps.gov.cn/n2254314/n2254409/n2254431/n2254438/c3697388/content.html

A 1999 commercial encryption regulation deemed all commercial encryption products as "state secrets" and prohibited the use of foreign encryption products.[23] 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 July 2019, the Government of China published a draft Cryptography Law for public comment.[24] BSA is concerned with the draft law for several reasons. First, it would subject commercial cryptography to import licensing and export control, without as yet any clear indications of the criteria by which licenses or export permission would be granted. This could significantly restrict foreign competition in commercial cryptographic products within the Chinese market. Additionally, the draft law lacks a clear definition of the scope of commercial cryptography — leaving significant uncertainty about which products and services would be subject to the licensing and export control regime.

Cross-Border Data Flows: 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.[25] In July 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.[26] 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 June 2019, the CAC issued draft Security Assessment Measures for Cross-Border Transfers of Personal Information for public comment.[27] The draft measures require all cross-border transfers of personal information to undergo a security assessment, and prohibit the cross-border transfer of personal information where the transfer is "likely to impact national security or impair public interests." 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 CSPs 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.

---

[23] *Regulation on the Administration of Commercial Encryption*, October 7, 1999 (Chinese) at: http://www.sca.gov.cn/sca/xxgk/1999-10/07/content_1002578.shtml

[24] *Cryptography Law of the People's Republic of China (Draft for Comment)*, July 5, 2019 (Draft Encryption Law).

[25] CSL, *op. cit.* Article 37

[26] *Critical Information Infrastructure Protection Regulations (Draft for Comment)*, July 11, 2017 (Chinese) at: http://www.cac.gov.cn/2017-07/11/c_1121294220.htm

[27] *Security Assessment Measures for Cross-Border Transfers of Personal Information (Draft for Comment)*, June 13, 2019 (Chinese) at: http://www.cac.gov.cn/2019-06/13/c_1124613618.htm

In November 2016, MIIT published a Draft Notice on Regulating Business Operation in Cloud Services Market (Draft Cloud Service Regulation Notice).[28] 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.[29]

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 require CSPs to construct and maintain physical 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 require the creation of duplicate copies of equipment, business systems, and data. This could make it cost-prohibitive and operationally impractical for foreign CSPs to operate in China, preventing them from participating on equal footing within the Chinese market and impeding their ability to partner on reasonable terms with Chinese companies.

Finally, while these policies themselves raise 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 2019, the CAC issued draft Cybersecurity Review Measures for public comment.[30] Under the measures, all "network products and services" purchased by critical information infrastructure operators will be subject to a cybersecurity review by the CAC. The measures do not define "critical information infrastructure" and could potentially require providers of products and services to provide access to valuable trade secrets and other IP, confidential commercial contract terms, and other sensitive information in order to pass the review. They also fail to specify what remedies are available for any wrong decisions made by the CAC. 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.[31] The MLPS, and its proposed successor scheme the CCPS,[32] impose significant restrictions on the procurement of software and other information security products for an overly broad range of information systems the government considers sensitive. Among other requirements, procurement 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, and in-country hosting requirements, as well as challenging processes for obtaining licenses and other prerequisites for entering the market.

---

[28] *Notice on Regulating Business Operation in Cloud Services Market (Draft for Comment)*, November 24, 2016, at: http://www.miit.gov.cn/n1146295/n1652858/n1653100/n3767755/c5381367/content.html

[29] Joint industry Association Comments on Draft Cloud Service Regulation Notice available at: https://www.bsa.org/~/media/Files/Policy/Trade/CloudRegComments.pdf

[30] *Measures for the Security Review of Network Products and Services (Interim),* May 24, 2019 (Chinese) at: http://www.cac.gov.cn/2019-05/24/c_1124532846.htm. Unofficial English translation at: https://www.tc260.org.cn/upload/2019-05-24/1558674533323034278.pdf

[31] MLPS, *op. cit.*

[32] CCPS, *op. cit.*

These restrictions are particularly acute for the telecommunications and IT industries, including cloud computing services.

Under China's Telecommunications Service Catalog[33] as read with China's telecommunications regulations, China imposes a host of market access restrictions on foreign firms which are not typically regulated as telecommunications service providers 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 telecommunications 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, which also apply indirectly the local partners of joint ventures.

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 (e.g. an individual company's proprietary product or services specifications) associated with foreign software products across a wide range of uses. Requirements to disclose source code and enterprise standards pose significant inherent risks to IP with little security value. It is critical that the United States intervene to eliminate current disclosure requirements and arrest further advancement of draft requirements.

The most significant measures relating to source code disclosure are found in the CSL, which includes requirements that products associated with CII be subject to security reviews.[34] Current implementing measures under the CSL contemplate that source code disclosures can be required as part of the security reviews but leave the specific mechanisms to future legislation.[35] 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 cryptography providers would be required to disclose source code to state licensers under the SCA's draft Encryption Law.[36]

Equally concerning are revisions to the Standardization Law enacted on November 4, 2017.[37] The revised law appears to require public disclosure of enterprise standards. Enterprise standards represent highly proprietary and confidential information that often is protected by trade secret law or other forms of IPR.[38] 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

---

[33] *Classification Catalogue of Telecommunications Services (2015 Edition)*, December 28, 2015 (Chinese), as revised in June 2019, at: http://www.miit.gov.cn/n1146290/n4388791/c69928928/content.html

[34] CSL, *op. cit.*

[35] Measures for the Security Review of Network Products and Services (Interim), *op. cit.*

[36] Draft Encryption Law, *op. cit.*

[37] *Standardization Law of the People's Republic of China*, November 4, 2017 (Chinese) at: http://www.npc.gov.cn/npc/xinwen/2017-11/04/content_2031446.htm. English translation at: http://www.cfstc.org/en/2932583/2968817/index.html

[38] China does not currently have a standalone trade secrets law, and trade secrets remain one of the most at-risk types of IP for US businesses operating in China. While companies 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 in Chinese courts 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.

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.

EUROPEAN UNION

Overview/Business Environment

Over the past five years, the European Union has modernized its digital economy regulatory and policy framework relevant to data service providers, in particular with regards to privacy, cybersecurity, data flows, and copyright. US data service providers expect this overhaul to continue as a new European Commission is set to take office late 2019. They are confronted with a growing rhetoric from the incoming EU leadership which aims to achieve EU's strategic autonomy and enhance its technological sovereignty. European authorities are considering measures that may constitute *de facto* market access barriers, i.a. in the area of data privacy, data sharing, artificial intelligence and competition. While BSA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, some of these policies could limit the ability of US firms to offer 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 service providers.

Market Access

As the incoming European Commission develops and implements new policy proposals, BSA asks that the United States 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.

Cross-Border 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 relating to any other market, such as China, South Korea, or Russia.

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 United States. 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. The Court held a public hearing on July 9th, 2019. The non-binding opinion of the Advocate-General is expected on December 12, 2019 and a decision on the case is expected early 2020.

In parallel, 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. Privacy Shield represents a strong agreement to foster transatlantic data transfers while safeguarding consumer privacy, as demonstrated by the number of companies certified to the program (over 4,900 in October 2019). Despite successful annual reviews (in 2017, 2018 and 2019), where the European Commission concluded that this framework continues to ensure adequate protection and safeguards for personal data transferred from the EU to the United States, Privacy Shield was immediately challenged before the EU General Court in cases brought by two privacy activist groups (Digital Rights Ireland and La Quadrature du Net). While the former has been dismissed, the latter has been admitted but put on hold until the CJEU rules on its above-mentioned case regarding the validity of Standard Contractual Clauses as a transfer mechanism.

In all these cases, the complainants contend that US practices on law enforcement and national security access to data lack sufficient privacy safeguards, and as such, the SCCs should be reviewed, and Privacy Shield should be invalidated. These legal challenges mean US companies will face continuing uncertainty in relying on the Privacy Shield and SCCs for transatlantic data transfers.

.

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, New Zealand, Chile, and Indonesia, in which it is intent on including this data flows language. The EU has also tabled this text as part of its proposal in the context of the WTO e-commerce negotiations.

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. Both the European Parliament and the Council have received their respective negotiating mandate, opening the way for trilogue negotiations to begin. The process is expected to conclude by end 2019.

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 about the wide-reaching and prescriptive rules included in the ePR and the narrow scope and number of exceptions.[39]

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.

On February 15, 2019, in order to facilitate further discussion among the Council, the Romanian Council Presidency published a revised text of the draft ePR. BSA continues to have serious concerns regarding the revised draft.[40]

In July 2019, BSA prepared an informal submission, answering the questions posed by the Finnish Presidency as preparatory work for the discussions in the Working Party on Telecommunications and Information Society on the ePrivacy Regulation.[41] As described at length in the submission, BSA highlighted the need to emphasize the importance of maintaining a clear distinction between the scope of the proposed ePrivacy Regulation and GDPR, and particularly the corresponding obligations they would establish. BSA also stressed the importance of ensuring the confidentiality of communications, the protection of personal data and a clear distinction between personal and non-personal data. BSA also urged the Council to better align the ePrivacy Regulation with Art. 6 of the GDPR and to thoroughly analyze the scope of the regulation and its possible overlap with GDPR. The Finnish Presidency has published an updated text on October 4th, addressing some of BSA priorities. Nevertheless, BSA continued to voice its concerns, most recently by joining a letter calling for a review of the whole proposal supported by a broad coalition of cross-sector associations

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

[40] Comments available at https://www.bsa.org/files/policy-filings/02262019balancedePrivacyRegulation.pdf

[41] Comments available at https://www.bsa.org/files/policy-filings/07042019eueprivacyquestionnaire.pdf

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, provide key cybersecurity services, and compete 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: (1) provisions governing funding and procurement; and (2) 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 a very positive development, during the Trilogue negotiations on the Copyright Directive, the Commission changed its approach to TDM and supported a broader mandatory exception to be enacted by all Member States. The final result of the negotiations was to confirm such an exception. The final text establishes an exception for TDM and allows rightsholders to reserve their rights against TDM activities through machine-readable means for content freely available online. The Directive was approved by Member States and the European Parliament in April 2019. Member States now have two years to enact legislation implementing the Copyright Directive, including a mandatory exception for commercial uses of TDM. The European Commission remains strongly supportive of the exception and is coordinating the work of Member States in the implementation of the Directive.

INDIA

Overview/Business Environment

The commercial environment for BSA members remains challenging in India.[42] In addition to certain policy and regulatory developments that may require data localization and hinder cross-border data flows, preferences for domestic products and services contained in certain procurement policies could restrict market access for BSA members.

The Committee of Experts[43] (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)[44] and the Personal Data Protection Bill, 2018 ('Bill')[45] to the Ministry of Electronics and IT (MeitY) in July 2018. This Bill has seen extensive debate, as it includes contentious provisions such as localization requirements for personal data and restrictions on the cross-border transfer of personal data. The Bill is expected to be introduced to Parliament in late 2019 or early 2020. In parallel to this important policy development, some sectoral regulators, including the Reserve Bank of India (RBI), have demonstrated support for data localization requirements. In February 2019, the Department for Promotion of Industry and Internal Trade (DPIIT) released a Draft National E-Commerce Policy which mandated several proposals which would pose substantial challenges that would restrict the ability to provide customers in India with the most seamless and secure digital services. The draft policy included data localization and restriction on data flows. The draft policy was later withdrawn given significant concerns from the industry. It is expected that a new draft policy would be released in 2020.

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.[46] 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, telecommunications, energy, and healthcare. Such policies do not offer a level playing field to US technology providers that are bringing cutting-edge technologies and services to India.

The existing and future software market in India remains at risk due to a variety of existing or proposed data localization requirements. From legacy policies on government-owned weather data,[47] to proposals regarding personal data, machine-to-machine (M2M) systems,[48] payment processing,[49] and existing public procurement

---

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

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

[44] *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians,* Report by Committee of under the Chairmanship of Justice B.N. Srikrishna (Expert Committee Report) (2018) at: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf

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

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

[47] Refer Section 2.1.d *Guidelines for Government Departments On Contractual Terms Related to Cloud Services* at: http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms_0.pdf

[48] *National Telecom M2M Roadmap (2015)* at: http://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

[49] *Reserve Bank of India Storage of Payment System Data Directive (2018)* at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0

requirements like the Make in India Order,[50] 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.[51] Rather, they weaken data security and unfairly disadvantage firms that provide or rely on global cloud computing services.

There appear to be positive developments with respect to the patentability of software-related inventions. In July 2017, the Office of the Controller General of Patents, Designs, and Trade Marks (CGPDT) issued Revised Guidelines for Examination of Computer Related Inventions Guidelines (2017 CRI Guidelines).[52] The Guidelines removed the "novel hardware" requirement for patent eligibility in patent applications relating to computer-related inventions. This is encouraging as it is in line with international practice, as well as India's Patent Law, and recognizes the possibility of software-enabled inventions receiving patent protection in India. It will be important to monitor how this revision is implemented in practice.[53]

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 software and information technology (IT) sectors in general.

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,[54] 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. 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.

Subsequently, MeitY issued the Draft Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products in furtherance of the Order for public comment.[55] In July 2018, MeitY issued the final notification with only minor changes.[56]

---

[50] Make in India Order, *op. cit.*

[51] *See section on 'Enhancing Cybersecurity',* BSA Cross-Border Data Flows, at: https://www.bsa.org/~/media/Files/Policy/BSA_2017CrossBorderDataFlows.pdf

[52] *Guidelines for Examination of Computer Related Inventions (CRIs); Office of the Controller General of Patents, Designs and Trademarks (2017)* at: http://www.ipindia.nic.in/writereaddata/Portal/Images/pdf/Revised__Guidelines_for_Examination_of_Computer-related_Inventions_CRI__.pdf

[53] *The Patents Act, 1970 (2005)* at: https://wipolex.wipo.int/en/text/295102

[54] Make in India Order, *op. cit.*

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

[56] *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

In our written comments on the Draft Notification to MeitY, BSA raised several concerns.[57] For example, the "local supplier" requirements under the Notification represent unfair barriers to 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.

The Notification and similar 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 opportunities.

Data Localization: There are a variety of examples where the Government of India has 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."[58] 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.[59]

The Directive on Storage of Payment System Data (Directive) issued by the Reserve Bank of India (RBI) on April 6, 2018, without any advance public consultation, imposes data and infrastructure localization requirements — requiring payment system operators to "ensure that the entire data relating to payment systems operated by them (system providers) are stored in a system only in India."[60] 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, voicing concern about these data localization requirements.[61] 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 to take against non-compliant firms. Furthermore, in early 2019, RBI notified banks that, according to its interpretation, the Directive is to be understood to apply to banks, in addition to payment processors, which has been causing additional market access issues to US companies.

The Expert Committee on Data Protection 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.[62] The Personal Data Protection Bill, submitted to MeitY by the Expert Committee at the same time, also contains problematic data localization requirements.[63] The Bill requires that data fiduciaries store in India "at least one serving copy" of personal

[57] BSA comments on the Draft Notification available at: https://www.bsa.org/~/media/Files/Policy/Data/10262017BSACommentsonIndiaMEITyDraftCyberSecurityProductsNotification.pdf

[58] Page 8 of 13 of *Guidelines for Government Departments On Contractual Terms Related to Cloud Services* (March 31, 2017) at: http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf

[59] Page 33 of 73 of *Invitation for Application/Proposal for Empanelment of Cloud Service Offerings* (May 2017) at: http://meity.gov.in/writereaddata/files/Application%20for%20Empanelment%20of%20CSPs.pdf

[60] Storage of Payment System Data Directive, *op. cit.*

[61] BSA Comments on RBI Storage of Payment System Data Directive, available at: https://www.bsa.org/~/media/Files/Policy/Data/06222018BSASubmissiontoReserveBankofIndia.pdf

[62] Expert Committee Report, *op.cit.,* Chapter 6 page 94

[63] Personal Data Protection Bill (2018), *op. cit.,* Chapter VIII, Section 40

data subject to the Bill. BSA submitted formal comments on this measure in September 2018, raising our concerns with the data localization provisions, among other things, in detail.[64]

In September 2019, MeitY also constituted a Committee of Experts to develop a governance framework for non-personal data or community data, which may result in polices requiring localization of non-personal data. It is expected that this Committee might also release a whitepaper for public consultation by the end of 2019.

One more example of how the Government of India seems to be aggressively promoting the concept of data localization is in the cloud computing policy environment. MeitY established the Working Group on Cloud Computing (Working Group) to look into policy issues concerning cross-border data flow and data security. Unfortunately, recent reports indicate that the Working Group may include broad data localization requirements for CSPs providing services both to the public and private sectors in its recommendations to MeitY.[65] The Working Group 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.[66] The recommendations have still not been published by MeitY and might eventually be released after the Personal Data Protection Bill is in the Parliament.

In February 2019, the DPIIT released a Draft National E-Commerce Policy, which contains several problematic proposals, which would restrict the ability of US companies to provide customers in India with the most seamless and secure digital services. Provisions requiring data localization and restrictions on data flows are particularly concerning. For the first time, the Draft policy also introduced the term called 'community data'. These discussions around 'community data' or 'non-personal data' later prompted MeitY to constitute a Committee of Experts on Non-Personal Data as discussed above. BSA submitted concerns regarding the Draft Policy in March 2019.[67] The policy was subsequently withdrawn, and it is expected that a new draft policy would resurface in 2020.

The United States should leverage mechanisms such as formal bilateral dialogues or potential trade agreements, 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.[68] 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.[69] 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.

---

[64] BSA Comments on India Personal Data Protection Bill available at: https://www.bsa.org/~/media/Files/Policy/Data/09282018BSACommentsonIndiaDataProtectionBill.pdf

[65] Kris Gopalakrishnan-headed panel seeks localisation of cloud storage data in possible blow to Amazon, Microsoft at: https://tech.economictimes.indiatimes.com/news/corporate/kris-gopalakrishnan-headed-panel-seeks-localisation-of-cloud-storage-data-in-possible-blow-to-amazon-microsoft/65278052

[66] 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

[67] BSA Submission on Draft National E-Commerce Policy at https://www.bsa.org/files/2019-03/03292019indiadraftecommercepolicy_0.pdf

[68] *Consultation Paper on Cloud Computing by Telecom Regulatory Authority of India, June 2016* at: http://main.trai.gov.in/sites/default/files/Cloud_Computing_Consultation_paper_10_june_2016.pdf

[69] BSA Comments on 2016 TRAI Cloud Computing Consultation Paper available at: https://www.bsa.org/~/media/Files/Policy/Data/07252016BSASubmissiononCloudComputingIndia.pdf

The TRAI then released its recommendations in August 2017.[70] 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 still unclear whether the TRAI is still considering potential server and data localization mandates.

Subsequently, the Department of Telecommunications released the National Digital Communications Policy — 2018 (NDCP 2018).[71] 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."

Privacy and Personal Data Protection: In July 2018, India issued the Personal Data Protection Bill prepared by the Expert Committee.[72] Although many aspects of the Bill would lay a strong foundation for a robust personal data protection framework if enacted, 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.[73] Since then, MeitY has been examining submissions from hundreds of stakeholders. A new version of the bill is expected to be introduced to the Parliament in late 2019 or early 2020.

In our comments, BSA describes our concerns that the Bill lacks the conceptual clarity and consistency that is crucial for the Indian digital economy to effectively integrate with the global data economy. In terms of regulatory capacity, although the Bill establishes an independent regulator called the Data Protection Authority, BSA is concerned this regulating body would not be properly resourced, would be asked to do too much, and may therefore 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.[74] Although the new version of the Bill has not been made public but we remain concerned that many of the troubling provisions remain unchanged, including the sections mandating data localization.

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.[75] 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.[76]

In December 2018, MeitY issued the Draft Information Technology [Intermediary Guidelines (Amendment) Rules] ("Draft Guidelines").[77] The Draft Guidelines include problematic filtering obligations that will create

---

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

[71] *National Digital Communications Policy 2018* at: http://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf

[72] The Personal Data Protection Bill (2018), *op. cit.*

[73] BSA Comments on India Personal Data Protection Bill, *op. cit.*

[74] *Ibid.*

[75] *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

[76] BSA Comments on TRAI Recommendations on Privacy, etc. available at: https://www.bsa.org/~/media/Files/Policy/Data/10302017BSACommentsonIndiaTRAIConsultationonPrivacySecurityandOwnerhipoftheDatainTheTelecomSector.PDF

[77] The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 – Draft available at: https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

significant privacy and data protection concerns for consumers. BSA has highlighted these concerns and urged MeitY to eliminate unnecessary obligations imposed on businesses. [78]

Intellectual Property

Requirement to Report on Patent Working – Form 27: This Form 27 imposes India-unique reporting obligations on patent holders and licensees and does not create any benefits. The form creates an enormous compliance burden on patent holders and an enormous administrative burden on the Controller General of Patents, Designs & Trademarks, diverting resources from innovation on the one hand, and other more useful administrative functions (such as examining patent applications) on the other. It also exposes patent holders to the risk that sensitive information may be revealed and to legal liability for unintentional errors or incompleteness. And it is effectively impracticable for patent holders, especially in the software-related technologies and services industries, that manage enormous patent portfolios and whose products and services are composed of an enormous number of patents, both owned and licensed, that interact in complex ways to result in value to the rights holders. BSA has submitted comments to the Government of India in March 2018[79] and July 2019[80]requiring the elimination of the form, or at least removal of some of the requirements it imposes but the status quo remains unchanged at this time.

[78] BSA Submission on Draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 available at: https://www.bsa.org/files/policy-filings/01312019BSAResponseDraftIntermediaryGuidelinesMeitY.pdf
[79] Comments available at https://www.bsa.org/files/policy-filings/03162018amendform27cgpdtm.pdf
[80] Comments available at https://www.bsa.org/files/policy-filings/06282019indiaamendform27dpiit.pdf

INDONESIA

Overview/Business Environment

The commercial environment for the software and IT sector in Indonesia is very challenging.[81] A variety of authorities have issued, or are in the process of developing, policies that will make, or threaten to make, it increasingly difficult to provide digital products and services to the Indonesian market.

Market Access

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."[82] 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.

Cross-Border Data Flows and Data Localization Requirements: The Government of Indonesia issued Government Regulation 82 of 2012 on the Operation of Electronic Systems and Transaction (GR82) in October 2012, and two implementing regulations under GR82 in subsequent years. These threatened data and IT infrastructure localization mandates.

In October 2019, the Government of Indonesia issued Government Regulation 71 of 2019 on the Operation of Electronic Systems and Transactions (GR71) to supersede and replace GR82. GR71 explicitly clarifies that public sector data must be managed, stored, and processed in Indonesia, but that there is no similar restriction on private sector data, which can be managed, stored, and processed anywhere, subject to requirements with respect to financial sector data that may be imposed by the financial sector regulator. The implications of the changes on business operations (especially with respect to public sector customers) are still to be determined. BSA recommends that USTR continue to work 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.

Source Code Disclosure Requirement: KOMINFO 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. If implemented, many global companies providing 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.

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

[82] *Regulation No. 17/PMK.010/2018 (Regulation 17)* (Indonesian) at: https://jdih.kemenkeu.go.id/fullText/2018/17~PMK.010~2018Per.pdf

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.[83] Korea has a strong IT market and a mature legal system. Over the past several years, however, the Government of Korea has adopted policies that have erected substantial market access barriers to foreign software 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[84] 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 industry sectors, such as government/public services, finance, healthcare, and education, hamper the ability to provide cloud-based services to users in these sectors.

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 software-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 very difficult for commercial cloud services providers (CSPs) to offer cloud services to entities in Korea's very broadly defined public sector. This is due to onerous certification requirements imposed by the Korea Internet Security Agency (KISA) on CSPs who provide cloud services to public sector agencies and requirements for physical network separation. Similar guidelines and regulations requiring physical network separation or data on-shoring apply to healthcare sectors.[85] Thus, even after enactment of the Cloud Computing Promotion Act, significant barriers to providing cloud computing and related services in Korea remain.

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. Physical network separation requirements prevent or discourage government agencies and other regulated sectors (e.g., healthcare) from adopting commercial cloud computing and related services.

On July 23, 2019 the Ministry of the Interior and safety (MOIS) and the Ministry of Science and ICT (MIST) announced revisions to Korea's Cloud Security Assurance Program (the Program).[86] The program requires that "the physical location of the cloud system and data shall be restricted to in county and cloud service area for public institutions shall be physically separated from the cloud service area for private institutions."

---

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

[84] *Act on the Development of Cloud Computing and Protection of its Users (Cloud Computing Promotion Act)* (2015). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#liBgcolor1

[85] E.g., under the Enforcement Decree of the Medical Service Act (Article 10-5: Standardization of Electronic Medical Records). Matters subject to standardization to be determined and publicly notified by the Minister of Health and Welfare pursuant to Article 23-2 (1) of the Act shall be as follows: "2. Facilities and equipment necessary for the safe management and preservation of electronic medical records under Article 23 (2) of the Act;"

[86] As announced at: https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939

As described in BSA's August 2019 comments, [87] this requirement will have a negative impact on Korea's digital ecosystem and curtail its ability to participate effectively in the global digital economy -- raising the cost of providing services and inhibiting the choice of technology available to end-users and procuring entities. The costs associated with such additional infrastructure will need to be recovered, which would ultimately increase the costs for end consumers.

The Regulation on Supervision of Electronic Financial Transactions (RSEFT)[88] was amended on October 5, 2016 to permit the use of cloud services by financial services institutions (FSIs). The amendment allows certain data to be stored on public cloud services. FSC recently approved the use of personal credit information by public cloud services and may be considering additional measures to expand the ability to manage financial data on the public cloud. However, FSC specifically requires that such data be maintained on servers located in Korea.[89]

Encryption: The proposed revisions to Korea's Cloud Security Assurance Program (the Program) that the Ministry of the Interior and safety (MOIS) and the Ministry of Science and ICT (MIST) announced in July 2019 requires that "cloud computing services providers shall use government-certified standard encryption technology when providing an encryption method for important material created through the cloud service." These kinds of national approaches to encryption, however, have limitations because of the global nature of the Internet, and the fact that criminal or terrorist acts are not limited by national borders. In fact, as outlined in BSA's comments, this kind of fragmented and piecemeal approach that only allows the use of domestically certified encryption standards may deprive organizations from using best-in-class encryption technologies, and this would weaken rather than strengthen the protection of sensitive data.[90]

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 are the Personal Information Protection Act (PIPA)[91] and the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act).[92]

Regulators and National Assembly members are currently reviewing Korea's PIP regime, partly in response to Korea joining the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) system and partly in response to the European Commission's interest in negotiating an "adequacy" recognition for Korea's personal information protection legal regime. Current legislative proposals would consolidate personal data protection provisions currently in the Network Act, the Credit Information and Protection Act,[93] and the PIPA into one law, the PIPA. Consequently, we understand that authority for interpreting and

[87] Comments available at https://www.bsa.org/files/policy-filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf

[88] *Regulation on Supervision of Electronic Financial Activities (RSEFT).* http://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B0%90%EB%8F%85%EA%B7%9C%EC%A0%95

[89] E.g., under RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.

[90] Comments available at https://www.bsa.org/files/policy-filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf

[91] *Personal Information Protection Act* (2017). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX

[92] *Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act)* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX

[93] *Credit Information and Protection Act* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX

enforcing personal information protection would be more completely under the responsibility of the Personal Information Protection Commission (PIPC), which may also become independent of the Ministry of Interior and Security (MOIS). The legislation may be considered by the National Assembly as early as the end of 2019.

These efforts at reform present 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.

In contrast to these promising developments, on August 29, 2018 the National Assembly passed a Bill amending the Network Act[94] requiring global companies without local presence in Korea to designate a representative with information protection duties in Korea and limiting onward transfers of personal information to third countries.

Domestic SME procurement in Public IT Network Equipment: The Ministry of Science and ICT (MSIT) enacted the Guideline of IT Network Equipment Installations in Public Sector (Guideline)[95] in 2017 to give preference to domestic small and medium-sized enterprises (SMEs). The Guideline significantly limits US suppliers' access to many public sector procurement opportunities, and they are inconsistent with Korea's international commitments. In 2018, MSIT proceeded to propose amendments to the Special Act on Promotion of Information and Communications Technology, Vitalization of Convergence Thereof, Etc. (ICT Special Act)[96] to provide a firmer legal basis for the Guideline. MSIT, in the explanatory note of the proposed legislative amendment,[97] stated that its intention is to raise the market share of domestic SME products in the public sector to a benchmark of over 96 percent (around 56 percent in 2017). This would match the share of SME products in the public sector software market in 2017.

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 certifications from accredited laboratories and should not impose further requirements for Common Criteria-certified products.[98] 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."[99] To make matters worse, a separate conformity test is required for each government agency, even for products procured and verified by another government agency.

This discriminatory application of security testing in public procurements to only international information security products also appears inconsistent with Korea's international commitments to national treatment and non-discrimination, including the US-Korea Free Trade Agreement (KORUS FTA). Although BSA and

[94] Partial amendment of Network Act. Bill Number [2015146].

[95] Guideline of IT Network Equipment Installations in Public Sector at: http://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/IT%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC%EC%9E%A5%EB%B9%84%EA%B5%AC%EC%B6%95%EC%9A%B4%EC%98%81%EC%A7%80%EC%B9%A8

[96] Special Act on Promotion of Information and Communications Technology, Vitalization of Convergence Thereof, Etc. at : http://elaw.klri.re.kr/kor_service/lawView.do?hseq=47794&lang=ENG

[97] "*Enhancing fairness on public ICT equipment procurement…MSIT, amending ICT Special Act*" at: http://www.etnews.com/20180614000322

[98] Common Criteria Recognition Arrangement (CCRA) at: https://www.commoncriteriaportal.org/ccra/

[99] *Ibid.*

other organizations have raised this issue several times with the Government of Korea, the issue remains unresolved.

While the Government of Korea has indicated that it intends to change the policy, it has not issued any formal correction in writing. It therefore remains unclear what the applicable requirements are.

More recently, the National Intelligence Services announced that it would enforce the new Korea National Security Evaluation Scheme in which all network vendors must meet 30 mandatory testing items from 2020. This outcome would reportedly favor domestic vendors that are not able to satisfy the CC certification that many US and foreign suppliers are able to meet. As noted above, Korea is a member of the CCRA and its departure from international norms in favor of country-specific norms is concerning.

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 RTG's 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.[100]

In addition, the persistence of high rates of unlicensed software use by enterprises continues to harm Thailand's software market. This is exacerbated by the widespread use of unlicensed software in the public sector.

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: In May 2019, Thailand enacted its Cybersecurity Act to strengthen the capabilities and authorities of government agencies to prevent, cope with, and mitigate the risk of cyber threats, especially with respect to critical information infrastructure. The Cybersecurity Act raises concerns as it gives the National Cybersecurity Committee (NCSC) broad powers to enter into premises, to monitor and test computers and computer systems, and to seize or freeze computers, computer systems, and equipment, without sufficient protections, such as opportunities to appeal or limit such access. 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 Thai market.[101] There is also criminal liability for organizations and individuals who do not comply with executive orders issued under the Cybersecurity Act.

Privacy: The Personal Data Protection Act (PDP Act) was enacted in May 2019 (on the same date as the Cybersecurity Act) and is Thailand's first omnibus legislation on personal data protection. 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.[102] It also heavily draws from the recently implemented General Data Protection Regulation (GDPR) of the European Union.

BSA's chief concerns with the PDP Act relate to prescriptive and burdensome notification and consent requirements for the collection, use, and disclosure of personal data. There are also potentially challenging breach notification requirements and liability for personal data breaches imposed on data processors.[103]

---

[100] *See generally*, BSA Cloud Scorecard – 2018 Thailand Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Thailand.pdf

[101] See BSA's comments, available at:
- https://www.bsa.org/~/media/Files/Policy/Data/05062015SubmissionCybersecurityBill_EN_DeputyPrimer.pdf;
- https://www.bsa.org/~/media/Files/Policy/Data/05212018enJointBSA_USABC_SupplementalCommentsThaiCybersecurityBill.pdf; and
- https://www.bsa.org/~/media/Files/Policy/Data/10122018EN_BSACommentsCybersecurityBillwith%20Annexes.pdf

[102] *APEC Privacy Framework* at: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework

[103] See BSA's comments, available at: https://www.bsa.org/~/media/Files/Policy/Data/03232015BSASubmissiononThaiPersonalDataProtectionAct_EN.PDF

VIETNAM

Overview/Business Environment

Over the past several years, Vietnam has enacted, implemented, and proposed various protectionist measures to regulate the software sector. These measures are likely to reduce fair and equitable market access for BSA members who wish to provide software products and online services in Vietnam.[104] The enactment of the Cybersecurity Law in June 2018, and current efforts to develop implementing rules, only exacerbate the existing challenges and threaten to make Vietnam an even less attractive destination for the delivery of cutting-edge software products and services.[105]

Market Access

Cybersecurity: On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the 20th version of the Cybersecurity Law (Law). The Law went into effect on January 1, 2019.

The Law raises serious concerns and will likely significantly impact the ability of many BSA members to provide software products and services in Vietnam. The breadth of the Law far exceeds cybersecurity protection and extends to a broad regulation of the Internet generally. The Law also grants vast powers to authorities and imposes stringent requirements on software product and service providers to comply with local cybersecurity standards and regulations and to apply for certification by local agencies. In sum, the Law is a significantly negative development in Vietnam's market access environment for the software sector. The Government of Vietnam has indicated its intention to issue regulations implementing the Law by the end of 2019. BSA submitted comments[106] on proposed implementing regulation aiming at minimizing the negative impact of the law. The latest draft implementing regulations suggest that the data localization and local presence requirements would only be implemented if a company fails to comply with a request under the Law from MPS. However, it is not clear what, if any, due process or judicial oversight may be available to companies that wish to contest an MPS order or penalties issued.

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 strengthening cybersecurity capabilities in Vietnam.

---

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

[105] *Vietnam National Assembly Passes the Law on Cybersecurity* (July 2, 2018) at: https://globalcompliancenews.com/vietnam-law-cybersecurity-20180702/

[106] December 13, 2018 comments available at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-implementing-law-on-cybersecurity. Joint comments by BSA and the US-ASEAN Business Council filed on September 12, 2019 available upon request.