October 26, 2021

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

Re: Request for Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers 86 Fed. Reg. 51436 (Sept. 15, 2021): Docket Number USTR–2021–0016

Dear Mr. Gresser,

BSA | The Software Alliance[1] provides the following information in response to your request[2] for written submissions to the Trade Policy Staff Committee (TPSC) regarding significant trade barriers for inclusion in the National Trade Estimate on Foreign Trade Barriers (NTE Report). The efforts of the Office of the US Trade Representative (USTR) to support open markets and combat trade barriers are critical to supporting global economic response and recovery to COVID-19. We look forward to any questions that you may have regarding our submission.

Sincerely yours,

Joseph Whitlock
Joseph Whitlock
Director, Policy
BSA | The Software Alliance

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

Submission of BSA | The Software Alliance re
National Trade Estimate on Foreign Trade Barriers

This document responds to USTR's solicitation of information relevant to the NTE Report, and contains the following major sections:

I. Executive Summary

The following executive summary introduces the importance of software and digital trade, relevant NTE criteria for digital trade, and key market access and intellectual property (IP) priorities in select economies.

A. Software and Digital Trade — Statistical Overview

Over the past decade, the US software industry and cross-border digital trade have become a primary driver of the global economy. As illustrated below, the US software industry has helped build stability and resilience into the US economy at a time of unprecedented economic uncertainty:

- Software drives growth: As of 2021, the US software industry (including US software exports) were responsible for $1.9 trillion of total US value added GDP and 15.8 million jobs — jobs that pay more than twice the national average for all occupations.[3]

- Software drives innovation: For example, BSA members are counted among the top US patent recipients (accounting in 2021 for nearly 75 percent of all US patents issued to US companies among the top 10 patent grantees)[4] and among the major US copyright and trademark holders. Annual US software research and development (R&D) investments exceed US$103 billion.[5]

- Software drives economic opportunity: Jobs in software development, computer programming and related fields are growing so rapidly that the US Bureau of Labor Statistics estimates 1 million computer programming jobs need to be filled in the United States.[6]

Internationally, these trends are also pronounced, and they have only accelerated in the wake of the COVID-19 pandemic:

- Digital trade drives the global economy: Pre-2020, software-enabled cross-border data transfers were estimated to contribute trillions of dollars to global GDP,[7] with 75 percent of the value of cross-border data transfers benefitting industries like agriculture, logistics, and manufacturing.[8]

- Digital trade is key to a global economic recovery: Post-2020, the shift to cloud- and software-enabled activity has accelerated. For example, the number of employees working remotely in mid-2020 is estimated to have grown (at least) four-fold over prior years,[9] while telehealth services are expected to grow seven-fold by 2025.[10]

Digital trade is the critical factor in global economic growth today. In every sector and at every stage of the production value chain, cloud- and software-enabled data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes to create jobs, boost efficiency, drive quality, and improve output.[11]

B. NTE Report Statutory Criteria and Policy Priorities for Software and Digital Trade

Unfortunately, trade barriers and digital protectionism are growing at the very time that digital trade and connectivity are helping to sustain economic activity and employment. Against this background, USTR's review of trade barriers under Section 181 of the Trade Act of 1974, as amended (19 USC § 2241), has ever greater salience. The statute requires 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.[12]

In this submission, we address all three statutory elements of Section 181 of the Trade Act as they relate to the trade-related challenges that BSA members increasingly face abroad, and as they relate to the trade-related aspects of BSA's COVID-19 Response and Recovery Agenda;[13] BSA's Digital Trade Agenda;[14] and BSA's Cloud Computing Scorecard.[15] Drawing on these BSA resources, BSA's NTE submission address policies of concern in the following markets: Brazil, China, India, Indonesia, South Korea, Thailand, Vietnam, and the European Union (EU).

C. Digital Market Access and Intellectual Property (IP) Issues in Select Economies

Both to recover from COVID-19 and to realize the full potential of digital trade, it is important to establish legal frameworks that foster innovation and promote confidence in the digital economy. BSA's Cloud Computing Scorecard examines the critical factors of such legal frameworks, 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 investment in software innovation and market access for software-enabled services and products.

1. Digital Market Access Issues

We highlight the following digital market access issues: (1) cross-border data flows and data localization; (2) discriminatory trade barriers including discriminatory digital taxes; (3) customs requirements on electronic transmissions; (4) security; (5) standards; (6) procurement restrictions, and (7) intellectual property rights (IPR).

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 restrict digital trade and market access. Data-related market access barriers take many forms. Sometimes the policies expressly require data to stay in-country or impose unreasonable conditions on sending data abroad. In other cases, the policies require the use of domestic data centers or other equipment, or the need for such data centers to be operated by local vendors. Sometimes these measures are based on privacy or security concerns, but too often the real motivation appears to be protectionist, as reflected in their design and operation. For example, these measures may:

- Reflect a choice of policy tools that are significantly more trade-restrictive than necessary to achieve the stated public policy goal;
- Constitute unnecessary, unjustified and/or disguised restrictions on data transfers across borders, or may be more restrictive of data transfers than necessary; or
- Treat cross-border data transfers less favorably than domestic data transfers.

Sustained attention to these threats is critical. Unfortunately, some markets, including **China, India, South Korea, Indonesia, and Vietnam**, have adopted, or have proposed, rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory.

China has published numerous measures that require data localization or restrict data transfers including the Data Security Law, the Personal Information Protection Law, and the Cybersecurity Law, as well as numerous subsidiary measures. India too has imposed data localization requirements, including through India's Directive on Storage of Payment System Data issued by the Reserve Bank of India in 2018, which imposes data and infrastructure localization requirements.[16] South Korea's Cloud Security Assurance Program (CSAP) requires use of local data centers for a broad range of cloud services.[17] The proposed implementation regulation for Indonesia's Government Regulation 71/2019 and OJK Regulation 13/2020 also contain data localization requirements. Likewise, Vietnam's 2018 Cybersecurity Law[18] and draft implementing regulations impose improper data localization requirements. These guidelines raise significant market access concerns for companies offering software, IT, and data services overseas.

Bangladesh,[19] **Egypt**,[20] **Nigeria**,[21] **Pakistan**[22] and **Saudi Arabia**[23] have also issued measures or proposals in that raise questions and potential concerns from a cross-border data policy perspective. Finally, BSA continues to monitor the application of measures in the **EU** that govern cross-border data flows, as well as the EU's bilateral and plurilateral trade negotiations and developing policies and legal jurisprudence, which could dramatically restrict cross-border data flows with third countries.

Discriminatory Trade Measures, including Discriminatory Digital Taxes: BSA members often face discriminatory measures in trading partner markets.[24] These measures include rules that afford less favorable treatment:

- To imported digital products vis-à-vis their domestic analogues in respect of sale, use, investment, technical regulations, etc.[25]
- To non-national services or service providers vis-à-vis domestic counterparts.[26]
- To digital products created in another country or by non-national relative to a digital protect created domestically or by a national.[27]

Similarly, such measures include discriminatory digital service taxes that would impose significant tax liability on US enterprise cloud and software providers, while effectively exempting local enterprise cloud and software providers. Such taxes would raise concerns under international trade law, insomuch as they would appear to constitute internal taxes or charges on imported products (imposed directly or indirectly) in excess of those imposed on like domestic products,[28] and/or taxes and charges applied so as to afford protection to domestic production.[29] For example, arbitrary value thresholds, definitional scoping, and other specific features that afford protection to domestic digital products, while burdening imported digital products, could raise concerns.

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 duties and other requirements on software and other electronic transmissions. 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."[30] Some countries, including **India** and South Africa, have also expressed support for the imposition of customs duties on electronic transmissions. If successful, these misguided efforts would increase costs of digital products and services and reduce productivity and competitiveness for local industries in the implementing countries.

Security: Governments have a legitimate interest in ensuring software-enabled products, services, and equipment deployed in their countries are reliable, safe, and secure. However, some markets — including **Brazil, China, India, South 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 instead ultimately hinders it. First, storing data at geographically diverse locations can enable companies to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location and obscure the location of data to reduce the risk of physical attacks. In addition, cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data.

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 or proposing de facto cybersecurity mandatory certification for ICT products, services and processes. The adoption of country-specific standards creates *de facto* trade barriers for BSA members and raises the costs of cutting-edge technologies for consumers and enterprises. Countries adopting nationalized standards for IT products include **China and South Korea**.

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 Australia, **China, South Korea, and India.**

2. Intellectual Property Issues

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. 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 South Korea** have implemented or proposed policies, such as sector-specific outsourcing or IT risk management frameworks, that require source code review of technologies or services.

Patents: BSA members depend around the world upon effective patent protection to eligible computer-implemented inventions, in line with their international obligations.

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, Internet service providers, 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.

Artificial Intelligence and Machine Learning: IP 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 data 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. Countries around the world are taking a range of approaches to modernize their legal frameworks for AI systems. This includes Japan's May 2018 Copyright Law Amendment Act ("the Act") and Singapore's January 2019 Copyright Review Report, which permit data analytics to be performed for both non-commercial and commercial purposes subject to requirements of lawful access — e.g. via a paid subscription.[31] The EU has also recently incorporated text and data mining exceptions to its copyright regime. Finally, in the United States, the "non-consumptive" reproductions that are necessary for the development of AI-related technologies are considered fair use. BSA urges the US government to continue promoting such AI-focused legal frameworks, including in countries like Australia[32] and **Brazil,** to foster innovation and creativity.[33]

Software License Compliance: The use of unlicensed software by enterprises and governments is a major commercial challenge for BSA members, having a commercial value of at least US$46 billion.[34] Unlicensed software also presents a serious security risk: Malware from unlicensed software costs companies worldwide nearly US$359 billion a year, and a single malware attack can cost a company US$2.4 million on average and can take up to 50 days to resolve. One means of mitigating these risks is through voluntary compliance measures, such as effective, transparent, and verifiable software asset management (SAM) procedures, where enterprises and government agencies implement the necessary processes to efficiently manage their software assets, including for licensing purposes. Governments should lead by example and adopt such measures for their own procurement and IT maintenance systems.

D. Conclusion

BSA welcomes the opportunity to provide this submission to inform the development of the NTE Report and the United States' engagement with important trading partners in 2022. 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.

II. Country-by-Country Analysis

A. Brazil

Overview/Business Environment

Although Brazil has taken positive steps to improve market access for cloud service providers, the overall market environment in Brazil remains challenging.

Market Access

Concerns about privacy and security have been used to justify some market access barriers for foreign software companies. This situation may, paradoxically, increase risks of security vulnerabilities and decrease Brazilian consumers' confidence that their sensitive personal data will be appropriately protected. In this regard, we continue monitoring the ongoing discussions about the about a National Cybersecurity Strategy, which have been led by GSI (the Cabinet for Institutional Security of the Presidency of the Republic), to ensure future cybersecurity regulations don't inadvertently create market access barriers.

Personal Data Protection Legislation*:* The Brazilian Congress approved the Brazilian Personal Data Protection Bill (known in Brazil as LGPD) in August 2018, and the law effectively came into force in September 2020. Legislation authorizing the creation of the Data Protection Agency (DPA) was approved in July 2019 and its structure was detailed through a Decree published in August of 2020. One of the provisions of the LGPD that requires implementation by the DPA is the one addressing international data flows. In particular, the DPA must implement several of the most important grounds for transferring data outside Brazil, including issuing adequacy determinations, approving standard contractual clauses, and approving global corporate rules (akin to Binding Corporate Rules). To ensure legal certainty, BSA has requested that the Brazilian issue interim guidance confirming that companies may continue to responsibly transfer data internationally based on global best practices that are consistent with the overall LGPD objectives.[35] To date, this guidance has not issued.

Data and Server Localization Requirements: The first Guidelines on Government Procurement of Cloud Services were issued in late 2018 and a newer version was issued in late August 2021 still including server and data localization requirements that will negatively impact the procurement of cloud computing services by all federal agencies.[36] The latest version of the Guidelines adequate the language to the Data Protection Law (LGPD) and add new concepts such as "cloud broker". BSA submitted comments on first draft guidelines urging Brazil to remove the localization requirements. However, Brazil did not adopt these recommendations, and the final Guidelines include the localization requirements.[37]

Copyright and Enforcement

The Brazilian Ministry of Citizenship is considering amendments to the current Brazilian Copyright Law. In July 2019, stakeholders were invited to comment on whether amending the law is necessary, and, if so, which provisions should be modified or added to the current law. BSA submitted comments suggesting the law be amended to add sections codifying notice and takedown, as well as provisions clarifying the permissibility of reproduction of content used for information analysis or research. The Ministry of Citizenship had announced it plans to issue a draft of the revised copyright law for public comment in early 2020, however, there have been no developments and the draft of the revised law is unlikely to be issued in 2021.

According to the most recent data, the rate of unlicensed software use in Brazil is 46 percent. This represents a commercial value of approximately US$1.7 billion in unlicensed software.[38] This is a far greater value of unlicensed commercial software than what has been measured throughout the rest of the region. Although recently improvements have occurred, BSA's enforcement programs in Brazil still

suffer from a very slow court system that prevents cases from being settled quickly and efficiently.

Notice and Takedown: Notice and Takedown is a process not currently codified by the Brazilian Copyright Law. Although the Brazilian Superior Court of Justice has once ruled that notice and takedown principles apply to assess internet provider liability, the ruling does not address the issue completely, and due to the nature of the Brazilian legal system, it is unclear how, if at all, the ruling would apply to other cases. It is, therefore, important that the issue by codified and the relevant provisions added to the revised Brazilian copyright law. We also noted in our comments that it is very important to ensure that the appropriate safe harbors are in place to protect ISPs from liability for copyright infringing content posted by third parties, and that such safe harbors should not be conditioned on any obligation by the ISP to monitor or filter infringing activity.

Information Analysis*:* In legal systems that do not have a flexible fair use provision, which is the case of Brazil, there can be some uncertainty about the permissibility of reproductions used for information analysis or research. It is therefore extremely important to create a specific data analysis provision to avoid any questions about the non-infringing nature of data analysis uses. This will help foster innovation through the continued use of data analysis for innovation purposes, without potential barriers that the threat of potential legal sanctions for copyright infringement could pose.

Compliance and Enforcement: BSA's enforcement program is based on civil cases brought against enterprises that use unlicensed or under-licensed software. In addition, BSA promotes voluntary compliance measures, such as effective, transparent, and verifiable SAM procedures, where enterprises conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed. BSA's efforts in Brazil also include a comprehensive educational communication campaign. This campaign is conducted exclusively online and is a collaboration with the local software association, ABES (Associação Brasileira das Empresas de Software). The campaign is meant to drive awareness of the risks of using unlicensed software.

BSA's relationship with the enforcement authorities in the past years improved due to increasing public awareness of IP-related issues. While civil cases continue to encounter court backlogs, judges in several major jurisdictions are responding well to requests for trials. Additionally, *ex parte* measures are available when necessary, and the courts order companies to cease using unlicensed software.

The Superior Court of Justice has reaffirmed earlier rulings that it is insufficient to simply order companies to pay the license fee they would have had to pay in the first place for the software they have been using without authorization. Instead, fines of multiple times the market value of the unlicensed software are being imposed. This provides greater deterrence in those cases that proceed to final judgment, but also sends a message to companies that they should not wait to be sued before legalizing their software use.

While these are positive trends, there is room for improvement. The Brazilian court system is generally slow. For example, in many instances, it may take anywhere from six to twelve months for an expert report to be ratified by the Court, allowing lawsuits to continue. In addition, Brazilian courts in certain cases continue to require high fees for forensic experts who conduct searches and seizures. Finally, court cases filed in the northern, northeastern, and midwestern regions of the country present additional challenges due to local judges' lack of IP expertise and the low number of qualified experts to perform inspections in those locations. The Ministry of Justice's National Council to Combat Piracy and Intellectual Property Crimes (CNCP) is the main governmental entity responsible for the central coordination and implementation of Brazil's national anti-counterfeiting and piracy campaign. It is critical that the CNCP be properly funded.

B. China

Overview/Business Environment

BSA members and other international technology providers face a particularly challenging commercial environment in China.[39] 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 efforts by the US and Chinese governments to achieve mutually beneficial solutions to these challenges.

China continues to present major market access challenges to BSA members. In 2017, the Government of China issued the Cybersecurity Law,[40] and followed it in 2021 with even more onerous cross-border data transfer restrictions and data localization requirements in the Data Security Law, the Personal Information Protection Law, and numerous subsidiary measures.

BSA urges the US Government 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

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 transfers and requirements to localize computing infrastructure.

BSA was pleased at the commitments negotiated by the United States and China in relation to cloud service purchases in the so-called “Phase One” trade agreement. The Phase One purchasing commitments included charges for the use of IP, which encompasses royalties for the computer software. More critically, the Phase One agreement contains purchasing commitments that cover “cloud and related services” under the IMF’s BMP6 Category, a critical area of economic activity for US services exporters that have faced a challenging investment and export environment for these services for many years. Covered services include: (1) data hosting, processing, and related services; (2) telecommunication services; (3) computer services; and (4) information services. At a time when both the US and Chinese economies are relying increasingly on cloud-enabled business environments (including via remote work, health and learning) to respond to the COVID-19 crisis, China and the United States have a shared interest in the fulfillment of commitments relating to computer software, as well as cloud and related services. BSA urges both countries to continue working towards fulfillment of those important commitments.

Unreliable Entities List regulation: On September 19, 2020, China’s Ministry of Commerce released the “Provisions on the Unreliable Entity List” (UEL).[41] The UEL, first proposed in May 2019, allow the Government of China to place foreign entities, which include non-Chinese companies, on an ‘Unreliable Entity List’ if they “endanger national sovereignty, security or development interests of China”, or “suspend normal transactions with an enterprise, other organization or individual of China,” or take discriminatory measures against such an entity. This can be done following an investigation or unilaterally. Once on the list, which will be public, restrictions could be placed on the activities of enterprises, organizations, and individuals in China. These include restricting import and export activities, restricting or prohibiting investment in China, banning entry or limiting travel of personnel related to the foreign entity, restricting or revoking work permits, imposing fines, and any other measure the PRC deem necessary. There is also no clear process for removing an entity. There is a high level of concern that the UEL could be used to justify imposing market barriers to companies for retaliatory or other purposes, unrelated to legitimate national security concerns.

***Law Countering Foreign Sanctions*:** On June 10, the National People's Congress approved the Law Countering Foreign Sanctions. The Law states that, "China has the right to take corresponding countermeasures" when another country "uses various pretexts or its own laws to contain or suppress China, take discriminatory restrictive measures against Chinese citizens and organizations, and interfere in China's internal affairs." It would appear to be within the scope of the broad authority granted under the Law to impose market access restrictions or other data-related restrictions.

Restriction on Cross-Border Data Transfers

The Government of China has put in place several laws and regulations restricting the free flow of data across borders and forcing data to be stored locally including the CSL. 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.

***Data Security Law*:** The Data Security Law ("DSL"), enacted on June 1, went into effect on September 1, 2021. The DSL (a) requires the State Internet Information Department to draft rules for all "other data handlers" (i.e., not just CII operators) to restrict those other handlers' exportation of "important data"; (b) applies to "[any person] handling important data"; (c) requires the State to create a "categorical and hierarchical system for data protection" as well as "catalog of" for "important data", and to assess the "importance" of data based on broad criteria relating to: economic development, social development, national security, the public interest, and the lawful rights and interests of citizens or organizations; (d) authorizes each region and department to set a "catalog of important data" within that region and in corresponding industries and sectors; and (e) requires the State to create a "monitoring and early warning system" for important data, which will apparently help it prevent the exportation of "important data" Following the swift enactment of the Data Security Law (DSL), the Cyberspace Administration of China and sectoral regulators such as the Ministry of Industry and Information Technology are already developing draft guidelines to establish the requisite frameworks for data categorization and classification under the DSL The implementing rules and guidelines for DSL have been identified as a work item under the State Council's 2021 Legislative Work Plan. As China begins work on classifying the scope of "important data" and other data classifications under the auspices of the DSL, it will be important to ensure that those categories of classification are not overbroad and do not automatically and improperly sweep in data categories, such as intra-company data transfers (e.g., of internal business and operational data) that are otherwise protected.

***Cybersecurity Review Measures*:** On July 10, the Cyberspace Administration of China ("CAC") published the draft Cybersecurity Review Measures ("Measures") for public consultation. The proposed amendments are primarily targeted at Chinese technology companies seeking an overseas IPO listing. The draft Measures has expanded its scope to require both Critical Information Infrastructure operators as well as data processors to go through a cybersecurity review. Among the new risk assessment criteria proposed in the draft Measures, they include:

- data security risks involving core data, important data, or a large amount of personal information being stolen, disclosed, destroyed, or illegally used or transferred across borders;
- critical information infrastructure, core data, important data, or a large amount of personal information will be affected, controlled, or maliciously used by foreign governments after listing abroad

***Personal Information Protection Law*:** On August 20, the National People's Congress of the PRC (NPC) officially released the approved version of the Personal Information Protection Law ("**PIPL**") which will take effect on November 1, 2021. Of particular concern are requirements for ex ante security assessments that impact data transfers that global companies have long engaged in for their daily business operations. The PIPL also raises the following concerns:

(1) data localization requirements for "personal information" (PIPL Art. 40) and highly restrictive data transfer provisions for "personal information" (PIPL Arts. 38-40);

(2) lack of definition or overbroad scope for key concepts that implicate data localization requirements and data transfer restrictions, including what constitutes a "justified need," or a "large volume [of data]" (PIPL Art 40);

(3) mandates for data assessments requiring governmental notification and/or approval in conjunction with the data localization and data transfer provisions noted above (PIPL Art. 38(1), 40);

(4) proposed data transfer "standard contracts" that, while encouraging, may not be interoperable with standard contractual clauses under the EU General Data Protection Regulation (GDPR) or other established personal data protection frameworks (PIPL, Art. 38(3));

(5) the absence from the PIPL of other internationally recognized data transfer mechanisms, such as intra-corporate binding rules, trustmarks and regional certifications (PIPL, Art. 38); and

(6) pre-transfer requirements for separate consent from individuals, even where another legal basis for transfer (such as contractual clauses) has been established. (PIPL, Art. 39).

(7) the ability for Chinese authorities to adopt retaliatory measures against overseas organization or individuals who have infringed upon the personal information rights and interests of any citizen of China, or endangered the national security or public interests of China (PIPL, Art. 42-43)

BSA and 31 other global associations raised these concerns in a letter submitted to China during the drafting process, but the concerns were not addressed.[42]

***Internet Medical and Health Information Security Management Specifications*:** The National Health Commission of the People's Republic of China has released a draft measures on Internet Medical and Health Information Security Management Specifications (国家卫生健康委统计信息中心关于征求《互联网医疗健康信息安全管理规范（征求意见稿）》标准意见). These draft measures contain data localization provisions modelled on the Data Security Law and draft Personal Information Protection Law. Similar to the approach taken in the Automotive Data Management Regulations, the measure requires storage of personal and important data in China, as follows:

> Personal information and important data collected and generated during the process and operation of Internet health care services should be stored in China. If, due to business needs, it is necessary to provide it abroad, a safety assessment shall be conducted in accordance with the methods formulated by the State Internet And Communications Department in conjunction with the relevant departments of the State Council, but if otherwise provided by laws and administrative regulations, it shall be administered in accordance with the relevant provisions.

***Automotive Data Management Rules; Connected Vehicle Data Security Requirements; Internet of Vehicles Data Rules*:** China has issued a range of restrictive data rules affecting the automotive sector. For example, the *Data Management Rules for Automotive Applications*, which became effective on October 1, 2021, require operators (e.g., automotive OEMs, etc.) to store personal data and important data in China. If strictly necessary, the operator may seek an exception from this rule based on an official approval for such transfer following a cross-border transfer security assessment conducted by government authorities. (ADMR, Art. 12). Operators are subject to strict legal obligations in connection with any transfer (supervising foreign data recipients; legal liability; data type, scope, use, and process limitations; governmental reporting requirements, etc.) (ADMR, Arts. 13-19). Similarly, under the *Connected Vehicle Data Security Requirements*, there is a strict prohibition of any cross-border transfer of Data relating to roads, buildings, topography, traffic participants, among others, and the vehicle location and track data, collected by a connected vehicle from the environment outside the vehicles through

cameras, radar and other sensors (CVSDR, Art. 7.1). Lastly, under the *Notice on Strengthening Internet of Vehicle (IoV) Cybersecurity and Data Security,* which are intended to support the implementation of the *New Energy Vehicle Industry Development Plan (2021-2035)*, ICV manufacturing enterprises and IoV service platform operation enterprises are required to conduct a cross border data transfer security assessment if they wish to provide important data abroad.

Cybersecurity Law: In November 2016, the National Peoples' Congress passed the Cybersecurity Law (CSL), which went into effect in June 2017.[43] The Cyberspace Administration of China (CAC) and other authorities continue to issue measures and standards to implement the CSL. Many of these measures leave important issues vague and unclear (e.g., the definition of critical information infrastructure (CII) or "important information"), or appear to expand the scope of the law — exacerbating the negative impact of these rules on the software industry. Broadly speaking, the impact of the CSL and related data regulations is to require that important information and personal information collected in China (by CII operators and others) must be held in-country.

Procurement

In January 2020, the Cybersecurity Review Measures became effective. Under the measures, all "network products and services" purchased by CII operators will be subject to a cybersecurity review by the CAC. The CAC can unilaterally trigger a review that can potentially be a disguised barrier to trade and market access, given the lack of transparent and object criteria and the wide discretion afforded to governmental authorities to deny approval. 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.

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. These restrictions are particularly acute for cloud computing services. For example, under China's Telecommunications Service Catalog and related measures,[44] China incorrectly classify a wide range of technologies and services as value-added telecom service (VATS) or basic telecom service (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 to local partners of joint ventures.

Standards and Technical Regulations

Cybersecurity Classified Protection Scheme: In May 2020, China posted the final version of the Cybersecurity Classified Protection Scheme (CCPS),[45] a de facto cybersecurity protection baseline for network operators and a universal compliance framework for the CSL. The CCPS is a continuation of the Multi-level Protection Scheme (MLPS).[46] Like the MLPS, the CCPS ranks the importance of network and information systems, based on their importance to China's national security, social order, public interests, and the legitimate interests of individuals and organizations and unnecessarily excludes access to foreign technology to the networks of moderate to high national importance — constituting a significant point of concern for the industry at large. The Government of China continues to release supporting standards and guidance on implementing the CCPS. For example, the September 22, 2020 "*Guiding Opinions on Implementing CCPS and CII Protection Scheme*"[47] which includes new concepts such as supply chain security and applies the CCPS to critical infrastructure protection. The CCPS came into effect on November 1, 2020.

Encryption: The China National Information Security Standards Technical Committee (TC-260) continues to release a myriad of draft cybersecurity standards involving encryption for public comment. A consistent and worrying trend exhibited by these standards is the extent to which they can be used to make it more difficult to participate in China's market, by creating a basis for favoring locally developed products over those developed outside of China. Such changes to algorithms or encryption mechanisms create technical barriers to trade and undermine interoperability.

In late 2019, the Government of China enacted the Cryptography Law.[48] BSA is concerned with the law for several reasons. First, while the updated Law states that commercial cryptography would not be subject to import licensing or export controls, the subsequent draft implementation regulations released suggest otherwise. Certification requirements for commercial cryptography are also being introduced. This overall regulatory framework could potentially restrict foreign competition in commercial cryptographic products. In implementation, it will also be important to avoid unwarranted source code disclosure requirements and to ensure that safeguards protect any trade secrets or other proprietary information. It is necessary for the USG to address the serious concerns of the software industry regarding privacy, security, and trade secret protection.

Intellectual Property

Over the past year, the Government of China has undertaken efforts to meet its IP-related obligations under the Phase 1 deal with the United States. These reforms have been conducted under three workstreams: (1) the "Plan for Promoting the Implementation of the Opinions on Strengthening Intellectual Property Protection (2020-2021)"[49] released in April 2020, (2) the "Plan of the Supreme People's Court for Initiation of Judicial Interpretation Projects for Year 2020"[50] released in March 2020, and (3) the "SPC released Opinions on Comprehensively Strengthening Judicial Protection of Intellectual Property"[51] released in April 2020.

Compliance and Enforcement: BSA and its members have had some success with China's IP Courts and tribunals. Unfortunately, we are observing capacity issues as the limited resources of those IP Courts and tribunals are tested against the growing backlog of cases. Given the positive experience BSA and our members have had with the existing system, BSA encourages the Government of China to establish additional specialized courts and provide more resources to the existing courts and tribunals.

Significant hurdles to effectively address the use of unlicensed software in China remain. In civil cases, most courts have relaxed excessively high burdens for granting evidence preservation orders, but others remain highly reluctant to issue such orders. Courts should also increase the amount of damages awarded against enterprises found using unlicensed software. China also needs to increase statutory damages beyond those currently proposed in the draft amendments to the Copyright Act.

The Criminal Case Transfer Regulations do not adequately address existing challenges to the effective transfer of administrative cases to criminal investigations and prosecution authorities. Some enforcement authorities have interpreted the regulations as requiring proof of illegal proceeds, rather than allowing transfer upon reasonable suspicion. Administrative authorities, however, do not employ investigative powers to ascertain such proof. We recommend that the regulations be updated to expressly include the "reasonable suspicion" rule.

C. European Union

Overview/Business Environment

Over the past several years, the European Union has modernized its digital economy regulatory and policy framework relevant to software and data service providers, in particular with regards to privacy, cybersecurity, data flows, and copyright. The new European Commission is actively pursuing an assertive digital policy agenda, guided by at times competing ambitions to promote Europe's "digital sovereignty" while pursuing "open strategic autonomy." The European Strategy for Data adopted in February 2020 clearly endorses that the EU will maintain an open, but assertive approach to international data flows and pledges that the EU will continue to address unjustified obstacles and restrictions to data flows in bilateral discussions and international fora. However, calls for data localization or for measures that seek to ensure EU organizations are immune from third countries' extraterritorial legislation continue to have traction at EU level and in some Member States, especially in the wake of the CJEU Schrems II decision and in light of the increased reliance on global digital technologies during the pandemic. While BSA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, and in harnessing the value of data, some of the measures considered, including in the areas of data privacy, cybersecurity, data governance, and cloud resilience in the financial sector (the so-called the 'Digital Operational Resilience Act' (DORA)), may constitute *de facto* market access barriers or dramatically hinder the ability of US organizations to move data across border.
The EU-US Trade and Technology Council can be an important asset to the transatlantic digital policy debate. BSA encourages both sides to use the TTC to exchange on common priorities and seek joint outcomes on *inter alia* Artificial Intelligence, data governance and international data transfers.

Market Access

As the EU co-legislators develop and implement new proposals, BSA asks that the US Government closely follow these developments, 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 historically focused on data transfers to the United States. The Commission has recently applied similar levels of scrutiny to the United Kingdom and the Republic of South Korea as both Third Countries sought an adequacy decision, but has not yet done so to data transfers relating to other markets such as China or Russia. It also has yet to evaluate existing adequacy decisions granted to markets including Canada, Argentina, Israel and Uruguay.

On July 16, 2020, the European Court of Justice in the Schrems II case invalided the EU-US Privacy Shield agreement. The Court also confirmed the validity of Standard Contractual Clauses (SCCs) which remain one of the main mechanisms under EU law to legally transfer personal data from the EU to third countries, especially in the absence of an adequacy decision. However, the Court also ruled that controllers and processors are required to verify, on a case-by-case basis, whether the law of the third country where the recipient is based ensures an "essentially equivalent" level of protection of the personal data transferred.

The Court decided that unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to SCCs, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country, including due to possible public authorities' access to that data.

In addition, the European Commission released a new set of SCCs in June 2021. The new set of SCCs contains general clauses that will be common to all future SCCs and in addition to the general clauses, controllers and processors should select between four different modules the most applicable to their situation. This is meant to allow the parties to tailor their obligations under the standard contractual clauses to their corresponding role and responsibilities in relation to the data processing at issue. The final SCCs anticipate that companies will assess the laws of the country to which data is transferred – and now specify that both the laws and "practices" of that country are relevant to such an assessment. Notably, the SCC implementing decision recognizes that companies may consider the absence of government access requests in their sector and their own practical experience in making these assessments. Paragraph 20 states that: "different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer." The final SCCs also make two meaningful changes on government access concerns by: (1) narrowing the circumstances in which notification to supervisory authorities is required, and (2) deleting the draft language that would have required companies to "exhaust all available remedies" to challenge a request.

Nevertheless, the implications of the Schrems II ruling continue to significant bearing on US companies that operate in Europe and / or act as service providers for customers in Europe. The ruling has added significant uncertainty with regards to the robustness and durability of the SCCs, a mechanism used by 90 percent of companies that transfer data internationally to some 180 countries. This uncertainty renders the conclusion of the negotiations of an enhance Privacy Agreement paramount to ensuring data can continue to flow across the Atlantic.

The complexities of the privacy framework underpinning personal data flows creates a gordian knot that trade policy should look to help detangle as quickly as possible. Once an agreement on an enhanced Privacy Shield is reached, the TTC should aim to formally incorporate aspects of international data transfers into its current discussions. Data transfers are critical to the success of many of the priorities set by the EU and the US in their respective policy agenda and to the TTC priorities.

France's Cloud Strategy: In July 2021, the French Government formally approved its Cloud Strategy for the public sector ("doctrine cloud de l'Etat"), which was announced earlier this year. The strategy aims at addressing the perceived lack of protection against cybersecurity threats and trust concerns related to Third Countries' governments access to data, and has been presented by government officials as a direct response to concerns highlighted by the CJEU in the Schrems II ruling.
While cloud services are essential to modernize the Government and the administration, the French government also suggests that when the administration chooses to rely on commercial solutions from the private sector (especially from French and European providers), they should bear in mind data protection principles and the localization of data in Europe.

The strategy revolves around the following axes:

- The strategy aims at developing a "cloud culture" by instituting automatic reliance on cloud services for new projects within the administration, and emphasizes that the use of commercial cloud services should be aligned with Gaia-X principles;
- When using a commercial cloud service to host/process sensitive data, the service will have to comply with 'Trusted Cloud' requirements, meaning obtain a certification from ANSSI (or an equivalent European qualification) and be immune to any extraterritorial regulation. At this stage the strategy document itself does not mention specifically where the data needs to be localized (in France or in the EU); early announcements mentioned that new types of partnerships, for instance through technology licensing so that foreign technologies licensed to EU companies, could also be eligible to that "Trusted Cloud label;
- The term "sensitive data" is only loosely defined as either personal data, economic data, or data related to the public administration.

Many questions remain which is raising some concern for non-EU providers. The Government has reiterated its commitment to this approach but has yet to offer full clarity on a number of important aspects of definitions and implementation of the Strategy.

Data Flows in Trade Agreements with Third Countries: In February 2018, the European Commission released data flows provisions for 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. This position is a positive step towards the EU endorsing binding trade commitments specifically focused on cross-border data transfers. However, it raises concerns due to its self-declaratory nature and potentially unlimited scope of exception with regards to privacy safeguards. At present the European Commission tabled this proposal in ongoing FTA negotiations with Australia and New Zealand, in which it is confronted to more advanced CP-TPP data flows provisions. The EU also tabled its language at the WTO Joint Statement Initiative talks on e-commerce.
In January 2021, the EU reached an agreement with the UK on digital trade provisions in the Trade and Cooperation Agreement governing EU-UK trade post-Brexit. The agreement translates for the first time in a trade agreement the EU's commitment to ensuring cross-border data flows to facilitate trade in the digital economy. While the agreed upon language on public policy exception remains further apart from more progressive provisions in USMCA or CP-TPP, it is considered by the European trade community as a positive step forward. Indeed, throughout 2020, several groups of Member States have repeatedly called on the Commission to adopt a high-level of ambition on data flows in the WTO e-commerce negotiations, even if it means diverging from the EU position as formally set by the negotiating directives. Similar letters have also called for an "open strategic autonomy" posture that preserves internal data flows in order to support the bloc's digital growth ambitions. By adopting forward-looking data flows provisions, the EU would be able to retain its influence on the multilateral stage and to continue to effectively push back against localization efforts in third countries. It would also bring it closer to its main trading partners—first and foremost the United States—and address some of the friction between trade and privacy following the CJEU Schrems II case.

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 European Union. 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.[52]

In October 2017, the European Parliament adopted its position on the draft Regulation. The Council has adopted its position in early 2021, including additional grounds for processing beyond the consent model for certain data categories, but largely maintaining the structure of the Regulation.

Trialogue negotiations between the European Commission, the European Parliament and the Council have begun in the Spring of 2021 and are ongoing. Not much progress has been achieved on the file, and BSA continues to express concerns on the structure of the proposal and on the very limited grounds for processing communications data.[53]

EU Cybersecurity Competence Centre: Following a proposal in September 2018, the EU Cybersecurity Competence Centre Regulation was formally adopted in May 2021. The regulation creates an EU Cybersecurity Competence Centre and Network (CCCN) 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 in the global cybersecurity market. As stated in the EU Cybersecurity Strategy released on 16 December 2020, "the CCCN should play a key role, with input from industry and academic communities, in developing the

EU's technological sovereignty in cybersecurity, building capacity to secure sensitive infrastructures such as 5G, and reduce dependence on other parts of the globe for the most crucial technologies." During the legislative process, BSA raised concerns with regards to the eligibility criteria of the CCCN in order to ensure that non-EU headquartered organizations and/or individuals would be eligible. The final language of Article 8 (3) reads as follows: "Only entities which are established within the Member States shall be registered as members of the Community." This language, coupled with a political willingness to support the emergence of a European domestic cybersecurity industry, could be interpreted to prevent subsidiaries of global companies from participating in the work of the Community and from benefiting from EU R&D funding instruments that will be governed by the Centre. However, the absence of a clear general definition under EU law of what it means for an entity to be "established" in the EU creates an uncertainty on whether a company that is headquartered outside of the EU, but that has one or multiple affiliates in Member States, is established in the EU and whether it is eligible to the CCCN.

Digital Operators Resilience Act (DORA): in September 2020, the European Commission adopted a new Digital Finance Package, which includes a proposal for an EU regulatory framework on digital operational resilience, the 'Digital Operational Resilience Act' (DORA). This proposed regulation aims at ensuring that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks. The proposed legislation will require all firms to ensure that they can withstand all types of Information and Communication Technology (ICT) - related disruptions and threats and the proposal introduces an oversight framework for ICT providers, such as cloud computing service providers.

This proposal, which builds on the European Banking Authority guidelines for outsourcing to cloud providers, could have potentially negative consequences for cloud computing service providers to financial services companies, and the current recommendations from the guidelines would become mandatory. Those would include, among others, the imposition of model contract clauses that would cover inspection and audit rights, termination rights and exit strategies; a new EU supervisory body to oversee large cloud providers, or large penalties for non-compliance. Moreover, Non-EU headquartered providers may be subject to higher levels of scrutiny.

D. India

Overview/Business Environment

The commercial environment for BSA members remains challenging in India.[54] 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 Government of India introduced the Personal Data Protection Bill, 2019[55] (PDP Bill 2019) to the Indian Parliament in December 2019. Although the PDP Bill 2019 reflects changes made to the previous version of the bill, a number of serious concerns remain. These concerns include requirements to localize critical data and to maintain copies of sensitive data in India (definitions of what type of data would constitute critical or sensitive data are not provided). The Committee of Experts' report to the Government on a Non-Personal Data Governance Framework, issued on July 12, 2020, proposes to require private enterprises to share non-personal data with the Central Government and competitors, among other issues.[56] Currently, a Joint Parliamentary Committee (JPC) is reviewing the PDP Bill 2019 and is potentially expected to table a report suggesting amendments by December 2021.

In parallel to these important policy developments, 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 requirements and restrictions on data flows. The draft policy was later withdrawn given significant concerns from the industry. It is expected that a new draft policy will be released in 2020. It is likely that the revised policy will retain localization requirements.

The Government of India is also working on the National Cyber Security Strategy (NCSS) that should be released in 2020. It will be important to ensure that the initiative promotes a robust cybersecurity environment in India while refraining from limiting the ability of companies to move data across borders or restricting companies' ability to encrypt data.

Government procurement policies remain outmoded and inefficient because of local content and technology preferences. In 2020, the Department of Industrial Policy and Promotion (DIPP) (now the DPIIT) revised the Public Procurement Order 2017 (Make in India Order), which requires government departments to give preference to local suppliers in procuring goods and services.[57] The Ministry of Electronic and Information Technology (MeitY)'s guidelines to government departments on cloud services contracts also contain requirements for data to be localized in India.[58] 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. Finally, India's framework for review and testing of certain IT products raises challenges to the ability of certain BSA members to certify or sell products in the Indian marketplace.[59]

The existing and future software market in India remains at risk due to a variety of existing or proposed data localization requirements. These requirements are included in various policies ranging from legacy regulations on government-owned weather data,[60] to proposed regulations on personal data protection, regulations on machine-to-machine (M2M) systems,[61] and payment processing regulations.[62] These policies do not promote security.[63] Rather, they weaken data security and unfairly disadvantage firms that provide or rely on global cloud computing services.

Market Access

The Government of India, at the central and state levels, has adopted a variety of policies negatively affecting the commercial environment for BSA members and the software and 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,[64] issued by the DIPP in June 2017 and revised in 2021, aims 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. By pegging procurement preference to 'local content', the order creates uncertainty and difficulty for foreign companies to participate in any government tenders/procurement processes.

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.[65] In July 2018, MeitY issued the final notification with only minor changes.[66]

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 Sovereignty*:* On September 2019, MeitY constituted a Committee of Experts to develop a governance framework for non-personal data (NPD framework). In August 2020, the Committee released its report, proposing a mandatory sharing and access framework for non-personal data. In our written comments on the non-personal data framework, BSA highlighted numerous concerns including mandatory sharing of proprietary non-personal data, restrictions on cross-border data flows and local storage requirements. Such mandatory obligations are counterproductive throughout the data ecosystem, and present additional complications if applied to "data processors," including enterprise software and cloud service providers. The framework proposes additional compliance obligations for businesses by creating a new regulator in addition to the proposed Data Protection Authority (DPA) under PDP 2019 and the proposed e-commerce regulator. The mandatory data-sharing framework proposed in the NPD framework is in addition to the sharing requirements proposed in the Personal Data Protection Bill 2019. These proposals have a chilling effect on innovation and investment in the digital economy.

Data Localization: There are a variety of examples where the Government of India has imposed, or proposes to impose, data localization requirements.

The PDP 2019 was introduced to Parliament in December 2019. Unfortunately, this version of the Bill continues to include seriously concerning provisions, including requirements to localize critical data (what constitutes critical data is not defined), to maintain copies of sensitive data in India (the definition of sensitive data is very broad and, in many cases, could not be separated from other types of data), and the grant of authority to the central government to require data fiduciaries and data processors "to provide any personal data anonymized or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed." BSA submitted formal comments on the 2019 Bill in 2020, raising our concerns in detail with the data localization provisions and other matters.[67]

In 2019, MeitY established the Working Group on Cloud Computing (Working Group). 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.[68]

Unfortunately, reports indicate that the Working Group may propose broad data localization requirements for CSPs providing services both to the public and private sectors in its recommendations to MeitY.[69] The recommendations have still not been published by MeitY.

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, as are the provisions related to "community data." BSA submitted concerns regarding the Draft Policy in March 2019.[70] The policy was subsequently withdrawn, and we expect that the DPIIT will issue a revised draft policy in 2020. It is likely that the revised policy will retain localization requirements.

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. MeitY again revised the empanelment invitation in 2020, under which it placed a strong emphasis on data localization. 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."[71] 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.[72]

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.

Privacy and Personal Data Protection: As mentioned above, MeitY presented the PDP Bill 2019 to the Indian Parliament in December 2019 for consideration and enactment. 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 our comments on an earlier version of the Bill, [73] 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, 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]

Unfortunately, as stated in the previous sections of this submission, the PDP Bill 2019 fails to address most of the concerns raised by BSA on the earlier, and it still includes many troubling provisions, including the sections mandating data localization and a new power allowing the government to compel disclosure of non-personal data upon request.

In December 2018, MeitY issued the Draft Information Technology [Intermediary Guidelines (Amendment) Rules] ("Draft Guidelines").[75] The Draft Guidelines include problematic filtering obligations that will create significant privacy and data protection concerns for consumers. BSA has highlighted these concerns and urged MeitY to eliminate unnecessary obligations imposed on businesses.[76] We expect MeitY to notify revised Draft Guidelines soon.

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.[77] 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.[78] 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.

The TRAI then released its recommendations in August 2017.[79] We were encouraged 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. Consequently, TRAI issued a Consultation Paper on cloud services in October 2019 seeking stakeholder comments. Among other things, this consultation paper discussed the modalities of an industry body to certify cloud computing services in India. The paper proposes a framework for such an industry body regarding registration requirements, membership, fees, and a code of conduct.[80] BSA submitted comments recommending that the TRAI should encourage the use and adoption of standards that are global, voluntary, and industry-driven and allow industry-bodies to be created voluntarily.[81]

In September 2020, TRAI released its 'Recommendations on Cloud Services’. Contrary to BSA’s inputs, TRAI recommends that a Department of Telecommunications (DoT)-registered industry body be formed for regulating CSPs. This policy process is now pending DoT action.

Intellectual Property

Compliance and Enforcement: The lack of statutory damages and inadequate damage awards in civil enforcement continues to be a challenge for BSA members when attempting to enforce their rights against enterprises using unlicensed software in India. Criminal enforcement has also not proven to be practical for enforcing against enterprise use of unlicensed software.

E. Indonesia

Overview/Business Environment

The commercial environment for the software and IT sector in Indonesia is very challenging.[82] 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

A variety of policies affecting the IT industry have been developed or proposed over the last several years that make, or threaten to make, it increasingly difficult to provide digital products and services to the Indonesian market.

Duties on Digital Products: In February 2018, the Ministry of Finance (MOF) issued Regulation 17, which amended Indonesia's Harmonized Tariff Schedule (HTS) to add Chapter 99 "[s]oftware and other digital products transmitted electronically."[83] 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 Transactions (GR82) in October 2012, and two implementing regulations under GR82 in subsequent years. These imposed data and IT infrastructure localization mandates.

In October 2019, the Government of Indonesia issued Government Regulation 71 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 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. Indonesia's reflection of the broad principle in GR71 that "private electronic systems operators" may place their systems and data outside of Indonesia is a positive development. This principle is important because the procedures and protections applied to ensure privacy, security, and investigatory access are more important to achieving these three objectives than the location at which the data is stored. Nevertheless, BSA remains concerned about new requirements for localization arising in implementation of GR71. The financial sector regulators (Bank Indonesia and OJK) continue to advance previous localization mandates with regards to private sector financial institutions that they regulate.[84] Implications of the changes on business operations (especially with respect to public sector customers) are still to be determined, particularly given the new e-Commerce regulation issued in November 2019, which seems to impact companies' ability to move personal data across borders (please see additional details below).

Personal Data Protection: Indonesia has been developing a draft Personal Data Protection (PDP) Bill since 2014. Based on BSA's reading of the draft Bill, it draws from several principles and aspects of the European Union's General Data Protection Regulation (GDPR), focusing on five main areas: data collection, data processing, data security, data breach, and the right for individuals to have their personal data erased. BSA's chief concerns with the draft Bill relate to potentially challenging breach notification requirements and liability for personal data breaches imposed on data processors. In terms of data

transfers, controllers are prohibited from transferring personal data outside of Indonesia unless one of four conditions is met: (1) the transfer is to a country or organization with a level of protection "equal or higher" than in the act, (2) there is an international agreement with the relevant country, (3) there is an agreement with the controller or a warranty that the controller will protect data in line with the act, or (4) consent of the personal data owner.

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.

E-Commerce Regulation: In November 2019, the Government of Indonesia issued GR80, a new e-commerce regulation. This regulation reportedly contains various concerning provisions relating to physical presence and registration. GR80 also imposes liability on foreign business actors and Internet intermediaries for content over which they lack direct knowledge or control. GR80 does helpfully clarify that this liability does not apply to intermediary service operators that (i) are mere conduits of information; (ii) only store data/information, either temporarily (caching) or for hosting purposes; and (iii) only act as search engine operators. It appears that cloud computing service providers, including enterprises offering SaaS, PaaS and IaaS solutions, would fall within the scope of this exemption from liability. However, a clarification to that effect could provide helpful guidance and avoid chilling investment and innovation in Indonesia.

Of particular concern to BSA member companies, are provisions in GR 80 that reportedly stipulate that personal data cannot be transferred offshore, unless the receiving nation is deemed by the Ministry of Trade as having the same level of personal data standards and protection as Indonesia. This requirement is overly restrictive, as it does not appear to account for other internationally recognized transfer mechanisms, including transfer pursuant to APEC CBPR System, or according to standard contractual clauses, binding corporate rules, certifications, marks, or other approaches. The measure should be amended to eliminate such provisions, or at least align with those of the draft PDP Bill.

F. Republic of Korea

Overview/Business Environment

The overall commercial environment in the Republic of Korea (South Korea) for BSA members and the software sector is mixed.[85] South Korea has a strong IT market and a mature legal system. Over the past several years, however, the Government of South 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 internationally recognized standards are available. Although the Cloud Computing Promotion Act[86] 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. These requirements may also be institutionalized by the National Assembly, with a bill recently proposed to create legal bindings to Cloud Security Assurance Program (CSAP).

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 South Korea. These policies 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 South Korea's very broadly defined public sector. This is due to onerous certification requirements imposed by the Korea Internet Security Agency (KISA) under the Cloud Security Assurance Program (CSAP) on CSPs that provide cloud services to public sector agencies and requirements for physical network separation. Similar guidelines and regulations requiring physical network separation or data onshoring apply to healthcare sectors.[87] Furthermore, we understand that certain non-government entities in the healthcare and education sector are now encouraged to adopt the CSAP, which has proven impossible for foreign CSPs to become certified. Thus, significant barriers to providing cloud computing and related services in South 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.

In 2016, the Ministry of the Interior and Safety (MOIS) and the Ministry of Science and ICT (MIST) adopted the CSAP, announcing certain revisions in 2019.[88] Since 2016, the CSAP has contained problematic physical network separation requirements.[89] As described in BSA's August 2019 comments,[90] these requirements will have a negative impact on South 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.

South Korea's regulatory environment for use of cloud services in the financial services sector has improved somewhat of late. The Financial Services Commission (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, the FSC specifically requires that such data be maintained on servers located in South Korea.[91]

Encryption: The revisions to the CSAP require 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. Cryptography certification also requires a review of source code, which could raise concerns regarding protection of proprietary information and trade secrets. 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.[92]

Personal Information Protection Regime: South Korea's personal information protection regime is one of the most stringent in the region and has significantly decreased the ability for BSA members to serve the South Korean market.

In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[93] the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act),[94] and the Credit Information and Protection Act.[95] The primary result of the legislative package is to consolidate the legal protection and enforcement provisions for personal information primarily in the PIPA, and to elevate the Personal Information Protection Commission (PIPC) to a central government-level agency under the Prime Minister.

The PIPA is currently undergoing another round of amendments. In September 2021, a revised PIPA Bill was approved by the State Cabinet, and it is now waiting to be tabled at the National Assembly. The amendments aim to move South Korea's personal information protection regime closer to that of EU's General Data Protection Regulation and may aid South Korea's efforts in attaining an "adequacy" recognition from the European Commission. However, more work is required to reform South Korea's personal data protection regime. There should be a clearer distinction between data controllers versus data processors to better delineate the roles and responsibilities of different entities. South Korea should also adopt measures that expand the legal basis for processing personal information beyond consent. This would enhance investment and innovation in emerging technologies, like data analytics and machine learning, while ensuring that personal information is appropriately and adequately protected.

Domestic SME procurement in Public IT Network Equipment: MSIT enacted the Guideline of IT Network Equipment Installations in Public Sector (Guideline)[96] 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 may be inconsistent with South 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)[97] to provide a firmer legal basis for the Guideline. MSIT, in the explanatory note of the proposed legislative amendment,[98] 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.[99]

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. In 2014, the Government of Korea extended similar security conformity testing requirements to international Common Criteria-certified networking products procured by any South Korean government agency.

South 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.[100] The additional requirements are in tension with the spirit of CCRA, which is to "eliminate the burden of duplicating evaluation of IT products and protection profiles."[101]

From 2020, the National Intelligence Services is enforcing the new Korea National Security Evaluation Scheme in which all network vendors must meet 30 mandatory testing items. This outcome would favor domestic vendors that are not able to satisfy the Common Criteria certification that many US and foreign suppliers are able to meet. Moreover, this security evaluation process is often delayed, sometimes for more than a year after the application, and there is no fixed deadline for completing the process.

Copyright and Enforcement

Compliance and Enforcement: Criminal enforcement has been an effective mechanism for BSA members to protect their rights and enforce against the use of unlicensed software by enterprises in South Korea. The police, the prosecutors' offices, and the special judicial police under the Ministry of Culture, Sports, and Tourism (MCST) are the authorities primarily involved in enforcement activities against enterprises using unlicensed software.

The special judicial police are specifically tasked with investigations and inspections concerning copyright violations and they are relatively active in conducting enforcement activities against enterprises using unlicensed software. However, they have limited resources and BSA members also rely on the enforcement actions of the police. In line with the Government of Korea's goal of reducing the rate of unlicensed software use, BSA recommends that the special judicial police increase its resources with a view to increasing the volume of enforcement activities against infringers.

BSA members also rely on civil litigation to take action against enterprises using unlicensed software. However, more can be done to improve the current system. For example, although preliminary injunctions are available, they are not often issued. It is also difficult to acquire evidence in civil cases without first going through a criminal raid. The option of aggravated damages is also not available to copyright holders under South Korean law. As a result, the damages awarded in civil cases tend to be too low to compensate rights holders or to deter future infringements. South Korea should amend the Civil Procedure Act, as the Supreme Court of Korea has suggested, to include effective discovery rules in civil cases.[102]

G. 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 enacted in 2019 — one on cybersecurity protection of critical infrastructure, and the other on personal data protection — are important elements of this effort, although the Government has yet to release implementing legislation for public consultation. BSA agrees that it is important for Thailand to have robust and effective cybersecurity and personal data protection legislation. However, we remain concerned that the implementation of both laws 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.[103]

Market Access

BSA shares the goals of the RTG's Digital Economy initiative, Thailand 4.0, and supports the thoughtful implementation of personal data protection and cybersecurity legislation. The RTG should, however, consider measures to minimize the potential unintended effects of recently enacted cybersecurity and personal data protection legislation that could 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.[104] There is also criminal liability for organizations and individuals who do not comply with executive orders issued under the Cybersecurity Act.[105]
In August 2021, the Ministry of Digital Economy and Society (MDES) issued a new Notification on "Criteria on Storing Computer Traffic Data of Service Providers B.E. 2564 (2021)" ("New Notification") to replace the previous Notification of Ministry of Information and Communication Technology Re: Criteria on Storing Computer Traffic Data of Service Providers B.E. 2550 (2007) (the "Previous Notification"). This Notification took effect on 14 Aug 2021 without any prior industry consultation, giving digital service providers only 180 days from this date to comply. The new regulation will require Data Centers and Cloud Service Providers to collect and retain extensive user information (e.g. identity info and activity logs) to facilitate authorities' access to users' data. This new regulation will increase compliance costs to both service providers and users, reduce competitiveness for small operators, and risk violating users' privacy rights.

Personal Data Protection: The Personal Data Protection Act (PDPA) was enacted in May 2019 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.[106] It also heavily draws from the General Data Protection Regulation (GDPR) of the European Union. BSA's chief concerns with the PDPA 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.[107]

In May 2020, the Thai Cabinet approved a royal decree granting a one-year exemption from certain provisions of the PDPA 2019 , which had been scheduled to take full effect on May 27, 2020. On 5 May 2021, the Cabinet decided to further extend the fully effective date of the PDPA under the Previous Royal Decree from 1 June 2021 to 1 June 2022. The provisions which are exempted include: consent requirements, notification requirements, establishment of lawful basis, requirements on the collection of personal data from other sources, and processing of minors' personal data. The enforcement of a second list of requirements is also postponed, including observance of data subjects' rights and data erasure or destruction requirements, the implementation of appropriate internal security measures to prevent unauthorized access, provision of data breach notifications, appointment of data protection officers (DPOs), filing complaints, and penalties.

The Personal Data Protection Committee which will be the implementing agency of the PDPA has yet to be established. This has held back work on the implementation of the PDPA, including the subordinate regulations that are meant to provide clarity over the implementation of the PDPA. In the interim, the MDES has conducted several focus group discussions with various stakeholders to work on the subordinate regulations.

Copyright and Enforcement

BSA enjoys good cooperation with RTG authorities, including with the Economic Crime Suppression Division (ECD) of the Royal Thai Police, in addressing unlicensed use of software in Thailand.

Compliance and Enforcement: Thailand has a specialized intellectual property (IP) court, which has improved the effectiveness of IP litigation in Thailand. Unfortunately, though damages awarded in civil litigation are occasionally reasonable, award amounts are very inconsistent and often inadequate to compensate the rights holder or deter future infringements. Expenses are often awarded, but only very small amounts, and they do not typically cover the actual legal costs. Preliminary injunctions are not granted regularly enough to be an effective tool. In addition, although criminal cases can be effective in Thailand, the courts should apply more deterrent penalties for convictions. In recent cases, courts imposed only a fraction of the potential fines or refrained from imposing any fines at all — simply suspending sentences — even in cases involving significant infringements.

H. 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 services in Vietnam.[108] 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.[109]

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 had indicated its intention to issue regulations implementing the Law by the end of 2019, but the implementing regulations are still pending. The latest draft of the implementing regulations was not released for public consultation and continued to have concerning data localization requirements. Although the draft Decree allegedly did not require foreign entities to store data in Vietnam, the draft gave the government the power to impose data localization and local presence requirements on foreign entities should a company fail to comply with a request under the Law from the Ministry of Public Security (MPS). It remains particularly concerning as these requirements can be applied irrespective of whether illegality is established, or a company has control over the data being used in violation, therefore posing a risk for Article 26 being triggered arbitrarily.

The draft also included a requirement for all local entities to store data locally. This is a concerning requirement that effectively enforces localization on foreign entities as a condition of doing business with local entities. These localization requirements remain a concern to the software industry at large.

***Personal Data Protection Decree*:** It is reported that Vietnam's Ministry of Public Security (MPS) has submitted its revised draft Decree on Personal Data Protection (PDP Decree) to the Ministry of Justice (MOJ) for internal appraisal. This current version of the draft Decree is kept strictly confidential during the internal appraisal and no copy of it is available. There are speculations that the MPS/MOJ may be able to submit the draft PDPD to the Prime Minister's Office for their review by the **end of September / early October**. The current targeted timeline for the draft Decree on Personal Data Protection to take effect is in **December 2021**.

Based on previous iterations of the draft PDP Decree, the PDP Decree will likely impose restrictive data transfer and data localization requirements. In addition, there are also additional burdensome requirements for personal data processors to store data transfer history for three years, register with the Personal Data Protection Commission (PDPC) for cross-border transfers of sensitive personal data with very detailed requirements for registration, and for the PDPC to carry out annual assessments or audit-like exercises on cross-border data transfers by personal data processors. These obligations are not only

impractical, they may also create new privacy and security concerns by forcing companies to store and access data they otherwise would not.

Draft Decree on Administrative Penalties in the Field of Cybersecurity: On September 23, the MPS also released a draft Decree on Administrative Penalties in the field of Cybersecurity, to be adopted on the basis of the Cybersecurity Law. Among others the draft details a number of infractions to the draft PDPD. The publication of this draft Decree, which is currently open for consultation, came as a surprise because the main PDPD is yet to be finalized. It does, however, provide insights in some of the key provisions under the PDPD such as data transfers, consent, data breach notification, etc. This draft Decree is expected to take effect in December 2021.

MIC Decisions 1145 and 783: In 2020, under the auspices of Vietnam's National Digital Transformation Strategy by 2025, the Ministry of Information and Communications (MIC) issued Decisions 1145 and 783 to announce a local cloud standard and cloud framework, respectively, for state agencies and smart cities projects. These measures may create a preferential framework for domestic cloud service providers , and measures currently characterized as "voluntary" will be treated as *de facto* requirements.

Decree 72: On July 6, the Ministry of Information and Communications (MIC) issued a draft decree to amend both Decree No. 72/2013/ND-CP (Decree 72) on the management, provision and use of internet services and online information and Decree No.27/2018/ND-CP (Decree 27) which amended and supplemented several articles in Decree No.72. The proposed amendments aim to allow the government to tighten control over livestreaming activities that generate revenue on social networks and impose obligations on cross-border social network service providers in Vietnam.

Not only does Decree 72 reinforce the data localization requirements found in other Vietnamese laws, BSA is also particularly concerned that the scope of covered entities could potentially include enterprise service providers even though many of the intended regulations are targeted at consumer-facing entities. There is also a new chapter under Decree 72 requiring providers of data center services to register with the MIC and contains additional obligations for data service providers to develop and implement technical plans and solutions to promptly detect and prevent illegal activities. These requirements place unnecessary and impractical burdens on data center service providers who may have to re-engineer their networks to afford them access to their enterprise customers' sensitive data which would be contrary to their contractual and other legal obligations.

Copyright and Enforcement

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code,[110] the Criminal Code,[111] and the Administrative Violations Decree.[112] The Civil Code operates in parallel.[113]

The Criminal Code criminalizes "commercial scale" acts of "[c]opying of works, audio recordings and visual recordings" or "[d]istributing the copies of work, audio or video recording." However, there has been a general lack of criminal enforcement against copyright infringement over the years by the relevant authorities.

On January 1, 2018, amendments to Vietnam's Criminal Code (adopted in 2015) went into effect.[114] The revised Criminal Code includes some improvements in provisions addressing copyright infringements. For example, there are several provisions applying criminal penalties for copyright infringements to commercial entities. Article 225 of the revised Criminal Code specifies that a commercial entity that commits copyright infringement is now subject to criminal penalties and may be fined up to VND3 billion (~US$150,000), and its business operations may be suspended for up to two years. However, the Government of Vietnam has yet to issue implementing guidelines in relation to how exactly Article 225 will be enforced. Such guidelines are required to clarify how Article 225 will supplement the existing regime.

Amendments to the Intellectual Property Code over the years have resulted in several improvements in the overall protection of copyright in Vietnam. However, more can be done to strengthen the legal framework for IP protection. BSA recommends introducing pre-established damages upon the election of the right holder, which can be very important in civil cases when the harm caused by the infringement is difficult to calculate.

Compliance and Enforcement: The lack of criminal enforcement against copyright infringement remains a concern. The general inactivity of the courts in dealing with copyright infringement issues also remains a problem in Vietnam. The Government of Vietnam should issue implementation guidelines on the enforcement of Article 225, which should clarify that the enforcement authorities and the courts are authorized and encouraged to prosecute criminal cases against commercial scale infringement, including against enterprises unlawfully using unlicensed software.

Also, there have been relatively few civil court actions involving copyright infringement in Vietnam. Complicated procedures, delays, and a lack of predictability in the outcome contribute to this problem. BSA remains hopeful that, over time, civil remedies will be available to supplement administrative, and eventually criminal, enforcement. However, the current difficulties in successfully bringing civil software copyright infringement cases coupled with a lack of clarity on how damages will be calculated for unlicensed software use has resulted in an increasing number of infringers being unwilling to settle cases with copyright holders despite clear evidence of rampant unlicensed software use. As a result, it remains challenging for copyright holders to obtain effective redress against infringers in Vietnam.

[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 30 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: BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] 86 Fed. Reg. 51436 (Sept. 15, 2021), at https://www.govinfo.gov/content/pkg/FR-2021-09-15/pdf/2021-19934.pdf

[3] Software.org, Software – Supporting US Through COVID (2021), available at: https://software.org/wp-content/uploads/2021SoftwareJobs.pdf

[4] IFI Claims Patent Services, 2020 Top 50 US Patent Assignees (accessed Oct. 11, 2021) ("2020 Top 50 US Patent Assignees"), available at: https://www.ificlaims.com/rankings-top-50-2020.htm

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

[6] BSA | The Software Alliance, *A Policy Agenda to Build Tomorrow's Workforce* (2018), available at: https://www.bsa.org/files/policy-filings/05022018BSAWorkforceDevelopmentAgenda.pdf.

[7] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), at https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.

[8] *Ibid.*

[9] *See generally,* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (2020), https://www.globaldataalliance.org/downloads/10052020cbdtremotework.pdf. Prior to the COVID-19 crisis between five and fifteen percent of US employees worked remotely. Today, studies indicate that 50 percent or more of employees are working remotely, with even higher percentages in certain regions and certain professions.

[10] *See generally*, Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (2020), available at: https://www.globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf.

[11] *See* Global Data Alliance, *The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector* (2020), at https://www.globaldataalliance.org/downloads/GDAeverysector.pdf ; See Global Data Alliance, *Jobs in All Sectors Depend Upon Data Flows* (2020), at https://www.globaldataalliance.org/downloads/infographicgda.pdf.

[12] 19 USC 2411 *et seq.*

[13] BSA | The Software Alliance, *Response and Recovery Agenda* (2020), at: https://www.bsa.org/files/policy-filings/05272020bsaresponserecoveryagenda.pdf.

[14] BSA | The Software Alliance, *Digital Trade Agenda* (2018), at: https://www.bsa.org/files/policy-filings/05072019bsa_advancingdigitaltradeagenda.pdf.

[15] BSA | The Software Alliance, *Cloud Computing Scorecard* (2018), at: https://cloudscorecard.bsa.org/2018/.

[16] *Reserve Bank of India Storage of Payment System Data Directive (2018)* at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0 and *Ministry of Electronics and Information Technology Guidelines for Government Departments on Contractual Terms Related to Cloud Services* at: https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.

[17] *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.

[18] *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.

[19] *See* Global Data Alliance, *GDA Comments on Bangladesh Draft Cloud Computing Policy,* May 12, 2021, at: https://www.globaldataalliance.org/downloads/05122021gdabdcloudpol.pdf

[20] In July 2020, Egypt enacted its first general privacy legislation, the Data Protection Law. The Law, which limits the grounds for data transfers, is due to take full effect following the passing of Executive Regulations.

[21] On 19 August 2020, the Nigerian Identification Management Commission published a draft Data Protection Bill. The Bill is intended to replace the existing Data Protection Regulation, issued by the Nigerian IT Ministry in 2018. The bill does not clearly establish the legal mechanisms for cross-border data transfers, which could engender regualtory uncertainty regarding an organization's ability to transfer data across international borders.

[22] In February 2020, Pakistan published a draft Data Protection Bill which includes two potential data localization requirements and which leaves key terms (e.g., scope of "critical data") undefined. The bill requires data mirroring for all personal data and local processing of all critical personal data , and prohibits the transfer of that data abroad. *See* Global Data Alliance, *Comments to the Ministry of Information Technology and Telecommunication of the Islamic Republic of Pakistan on The Personal Data Protection Bill 2020* (May 15, 2020), at www.globaldataalliance.org/downloads/051420pakistanpdpbill.pdf

[23] On September 24, 2021, Saudi Arabia published a new Personal Data Privacy Law (PDPL), which will become effective March 23, 2022. Companies must bring themselves into compliance by March 2023. Article 29 of the PDPL reportedly contains strict cross-border data restrictions – namely that "except in cases of extreme necessity relating to a threat to the life of the data subject, controllers may not transfer personal data outside the Kingdom unless the transfer is required to comply with an agreement to which the Kingdom is party, to serve Saudi interests, or for other purposes set out in the executive regulations, provided that a series of strict conditions set in Articles 29(1)-(4) are met. *See generally,* OneTrust Data Guidance, Saudi Arabia: New Personal Data Protection Law – What you need to know (Sept. 2021), at: https://www.dataguidance.com/opinion/saudi-arabia-new-personal-data-protection-law-%E2%80%93-what

[24] *See e.g.,* India Equalization Levy (as amended April 2020); Indonesia Electronic Transactions Tax (2020); Vietnam Tax Administration Law (July 1, 2020).

[25] *See* GATT Art. III:4, TBT Art. 2.1, TRIMS Art. 2.1; etc.

[26] *See* GATS Art. XVII.

[27] *See e.g.,* USMCA Art. 19.4.

[28] *See* GATT Art. III:2.

[29] *See* GATT Art. III:1.

[30] 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."

[31] 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.

[32] The copyright regime in Australia does not have an exception allowing the use of text and data mining for the purposes of develop AI algorithms. The current round of copyright reforms in Australia failed to address the private sectors' concerns and focused on non-commercial and government use exceptions. They are detailed at: https://www.communications.gov.au/departmental-news/copyright-access-reforms.

[33] 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.

[34] See BSA Global Software Survey – In Brief (June 2018), available at: https://gss.bsa.org/wp-content/uploads/2018/06/2018_BSA_GSS_InBrief_US.pdf.

[35] https://www.bsa.org/files/policy-filings/09092020bsagdalgpdimplement.pdf.

[36] https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684

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

[38] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at http://www.bsa.org/globalstudy. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2017 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[39] 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.

[40] *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/

[41] *Provisions on the Unreliable Entity List*, September 19, 2020, at: http://english.mofcom.gov.cn/article/policyrelease/questions/202009/20200903002580.shtml.

[42] Multi-association Letter on Draft Personal Information Protection Law and Draft Data Security Law, June 2, 2021, at: https://www.globaldataalliance.org/downloads/en06022021gdachinadslpip.pdf

[43] CSL, *op.cit.*

[44] *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.

[45] *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.

[46] *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.

[47] *Guiding Opinions on Implementing CCPS and CII Protection Scheme,* September 2020 (English) at: https://www.mps.gov.cn/n6557558/c7369310/content.html.

[48] *The Cryptography Law of the People's Republic of China*, December 2020 (Chinese), at: http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml; *China's New Cryptography Law – Still No Place to Hide,* December 2020, at: https://www.chinalawblog.com/2019/11/chinas-new-cryptography-law-still-no-place-to-hide.html#:~:text=The%20PRC%20National%20People%27s%20Congress,effect%20on%20January%201%2C%202020.&text=The%20Law%20provides%20that%20it%20welcomes%20foreign%20providers%20of%20commercial%20encryption.

[49] *Plan for Promoting the Implementation of the Opinions on Strengthening Intellectual Property Protection (2020-2021), April 2020, (Chinese), at:* http://www.cnipa.gov.cn/zscqgz/1147678.htm.

[50] *Plan of the Supreme People's Court for Initiation of Judicial Interpretation Projects for Year 2020,* March 2020 (Chinese), at: https://mp.weixin.qq.com/s/Z8vPkL7T_zOVfniNBm9qEw.

[51] Opinions on Comprehensively Strengthening Judicial Protection of Intellectual Property, April 2020 (Chinese), at: https://mp.weixin.qq.com/s/7Tm6l40Pg0htd7lS0gbRJQ.

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

[53] Comments available at: https://www.bsa.org/policy-filings/eu-bsa-policy-recommendations-on-the-eprivacy-negotiations. .

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

[55] *Personal Data Protection Bill, 2019* at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[56] *See* Report on Non-Personal Data Governance Framework by the Committee of Experts at: https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

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

[58] *Guidelines for Government Departments On Contractual Terms Related to Cloud Services* at: https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.

[59] Measures of concern to certain BSA members that produce IT products include:

- Draft Indian Telecom Security Assurance requirements (ITSAR) announced in early 2020 include source code review provisions that raise concerns regarding the protection of proprietary information. The draft also deviates from risk-based cybersecurity management practices (e.g., *see* provision on production of software free of all known vulnerabilities and provisions for recertification/retesting for every update, model upgrade or hardware change, without any distinctions.
- The Mandatory Testing & Certification of Telecom Products (MTCTE) framework announced in September 2017 presents challenges due to the lack of testing infrastructure in India, India's reluctance to accept international certification, and a three-month timeframe for tests.
- The Communication Security Certification Scheme (ComSec). Originally, security testing was part of the overall MTCTE, but it is now covered under ComSec, meaning that two separate certifications will be required for the same product.
- The Compulsory Registration Order (CRO). The CRO, which prescribes safety standards and in-country testing requirements for ICT products, just entered Phase 5 of its implementation. The CRO reportedly raises concerns about delays in product registration and duplication of tests.

[60] 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.

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

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

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

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

[65] *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.

[66] *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.

[67] BSA Statement on India's Personal Data Protection Bill, at: https://www.bsa.org/news-events/news/bsa-statement-on-indias-personal-data-protection-bill.

[68] 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

[69] 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

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

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

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

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

[74] *Ibid.*

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

[76] BSA Submission on Draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 available at: https://www.bsa.org/files/policy-filings/01312019BSAResponseDraftIntermediaryGuidelinesMeitY.pdf

[77] *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

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

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

[80] Consultation Paper on Cloud Services, October 2019, accessible at: https://www.trai.gov.in/sites/default/files/CP_23102019.pdf

[81] Comments available at: https://www.bsa.org/files/policy-filings/11202019indiatraicloud.pdf

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

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

[84] See OJK 013/2020.

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

[86] *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.

[8787] On June 1 of 2020, a new certification framework that includes CSAP requirements was applied to electronic medical records. *See* Enforcement Decree of the Medical Service Act (Article 10-5: Standardization of Electronic Medical Records) (indicating that "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").

[88] *See* https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939.

[89] As of the 2019 amendments, the physical network separation requirements stipulate that, "the physical location of the cloud system and data shall be restricted to in country and cloud service area for public institutions shall be physically separated from the cloud service area for private institutions."

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

[91] 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.

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

[93] *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.

[94] *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.

[95] *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.

[96] 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.

[97] 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.

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

[99] Similar concerns arise in the case of more recent public sector procurement initiatives. The "Korean New Deal" project announced in July 2020 foresees investment of KRW 160 trillion (USD 133 billion) by 2025 to stimulate the Korean economy after the COVID-19 pandemic. This investment includes a KRW 300 billion (USD 266 million) financial infusion to help domestic small and medium-sized enterprises transform themselves into digital enterprises. Foreign companies are reportedly excluded from bidding for projects to provide solutions for building a non-face-to-face working environment. Additionally, South Korea plans to install gigabit speed Wi-Fi in 200,000 schools nationwide by the first half of 2021, but the authorities reportedly demand the use of more than 50% of domestic parts in key Internet access points. *See,* 300 billion new markets for non-face-to-face solutions...Competition in South Korea's SW industry is heating up, at: https://n.news.naver.com/article/030/0002899498. Open a digital New Deal? Entrance barrier to school Wi-Fi, at: https://www.sedaily.com/NewsView/1Z93AOBUP9.

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

[101] *Ibid.*

[102] *Civil Procedure 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

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

[104] 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

[105] In addition to the foregoing measures, the Ministry of Digital Economy and Society (MDES) also issued a so-called Emergency Decree on Electronic Meetings, stipulating that electronic meetings on confidential matters must be conducted through a meeting control system established within the country. As reported, this measure raises concerns about its ambiguity, as well as concerns regarding the imposition of such a local development condition.

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

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

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

[109] *Vietnam National Assembly Passes the Law on Cybersecurity* (July 2, 2018) at: https://globalcompliancenews.com/vietnam-law-cybersecurity-20180702/. Another measure that we continue to monitor is Vietnam's Outline of Draft Decree on Personal Data Protection, which was published for public comments earlier this year, contains registration requirements for processing of sensitive personal data and transfer of personal data of Vietnamese citizens overseas.

[110] *Law on Intellectual Property (No. 50/2005/QH11) (IP Law)* (2006). English translation at: https://wipolex.wipo.int/en/text/274445

[111] *Criminal Code (No. 100/2015/QH13)* (2016) at: https://wipolex.wipo.int/en/text/446025. English translation at: https://wipolex.wipo.int/en/text/446020

[112] *Decree No. 131/2013/ND-CP on Sanctioning Administrative Violations of Copyright and Related Rights*, entry into force December 15, 2013 (replacing Ordinances No. 47 and 109) at: https://thuvienphapluat.vn/van-ban/So-huu-tri-tue/Decree-No-131-2013-ND-CP-on-sanctioning-administrative-violations-of-copyright-and-related-rights-212865.aspx.

[113] *Civil Code (No. 91/2015/QH13)* (2017) at: https://wipolex.wipo.int/en/text/445451. English translation at: https://wipolex.wipo.int/en/text/445414

[114] *Law No. 12/2017/Q14 (Amended Criminal Code)*, see *Vietnam: 2015 Penal Code to Take Effect on 1 January 2018* at: https://globalcompliancenews.com/vietnam-new-penal-code-20171110/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original