SPECIAL 301 SUBMISSION

February 6, 2020

Docket No. USTR-2019-0023

Jake Ewerdt
Director for Innovation and Intellectual Property
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Dear Mr. Ewerdt,

BSA | The Software Alliance[1] provides the following information in response to the notice published by the Office of the U.S. Trade Representative (USTR) seeking comments on the 2020 Special 301 review under the Trade Act of 1974 ("Special 301").[2]

Pursuant to the Special 301 statutory mandate, Section 182 of the Trade Act of 1974, as amended by the Omnibus Trade and Competitiveness Act of 1988 and the Uruguay Round Agreements Act of 1994 (19 USC § 2242), requires USTR to identify countries based on two separate sets of criteria:

- "Those foreign countries that **deny adequate and effective protection of intellectual property rights**, ***or***
- **Deny fair and equitable market access to United States persons that rely upon intellectual property protection**" (emphasis added).

In this submission, we address both elements of Section 182 of the Trade Act. The document highlights US trading partners with **deficiencies in protecting and enforcing intellectual property rights** *and* US trading partners that have erected **unfair market access barriers** that affect BSA members. For some countries, the market access barriers present the higher threat to BSA members' ability to do business in the market. In other cases, US trading partners are deficient on both counts.

[1] BSA's members include: *Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.*

[2] https://www.regulations.gov/document?D=USTR_FRDOC_0001-0566

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

Software has a profound impact on the American economy. According to a recent study from Software.org: the BSA Foundation,[3] the US enterprise software industry has expanded nearly twice as fast as the overall US economy in the past three years. According to the same study, software contributed more than $1.6 trillion to US value-added GDP in 2018 — a 19.1 percent increase in two years. The software industry supports 14.4 million jobs in all sectors of the economy and throughout the United States, and it employs 3.1 million people directly. BSA members are among the top US patent recipients and the software industry invested more than $82.7 billion in research and development (R&D) in the United States in 2016. These investments in intellectual property (IP) and innovation help make software a powerful catalyst for economic change — making businesses more competitive and the US economy more prosperous.

BSA members rely heavily on **open access to US trading partners' markets**; the adequate and effective protection and enforcement of **patents, copyrights, and trade secrets**; and legal frameworks of **intellectual property rights (IPR) exceptions and limitations** — consistent with US law. These rights have been critical drivers of US leadership in innovation and creativity, and US exports and job creation, in the digital economy. Innovative US companies operating internationally depend upon cross-border data transfers and global digital delivery models to realize a return on investments in R&D and to commercialize their IPR. Increasingly, market access barriers in trading partner markets take the form of policies that restrict a company's ability to transfer data outside a country where it is collected.

BSA members also face significant challenges due to the availability and extensive use of unlicensed software products, especially **unlicensed use of software** products or services **by governments, state-owned enterprises (SOEs),** and **business entities.**

In the following sections, BSA provides specific country reports on US trading partners that do not provide **fair and equitable market access** to BSA members, fail to provide **adequate and effective protection of intellectual property**, or both. We recommend these countries be listed on USTR's Priority Watch List or Watch List. We also request that the European Union (EU) be noted in the report as a Region of Concern due to increasing market access barriers that impact BSA members' ability to compete effectively in that market.

BSA recommends that the following countries be identified in the Special 301 report:

Priority Watch List:	**Chile, China, India, Indonesia, and Vietnam**
Watch List:	**Argentina, Brazil, Korea (Republic of Korea), Mexico, and Thailand**
Region of Concern:	**European Union**

Market Access and Intellectual Property Issues

To realize the economic promise of software, cloud computing, and emerging technologies, it is important to establish a legal framework that fosters innovation and promotes confidence in the digital economy. We highlight key market access and intellectual property issues below. The country reports immediately following this introduction set out BSA's specific concerns.

Cross-Border Data Flows and Data Localization: The ability of US companies to continue leading global advances in innovative technology is under a rising threat from foreign government policies that hamper US business models and hinder the international movement of data. Data-related market

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

access barriers take many forms. Sometimes they expressly require data to stay in-country or impose unreasonable conditions in order to send it abroad. In other cases, they require the use of domestic data centers or other equipment. Sometimes the barriers are based on privacy or security concerns, but too often the real motivation is protectionism, as the policy means chosen are often significantly more trade-restrictive than necessary to achieve any legitimate public policy goal. Immediate attention to these threats is urgently needed. Unfortunately, some markets, including **China, India, Indonesia, and Vietnam** have adopted or proposed rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory. BSA also continues to monitor developments in the **European Union** that could restrict cross-border data flows and pose significant market access barriers.

Measures that impede cross-border data flows and mandate data localization requirements are gravely disruptive to international trade. BSA urges the US Government to work with its trading partners to prevent or remove such practices and leverage all available trade mechanisms, including Special 301, in that respect.

Security: Governments have a legitimate interest in ensuring software products, services, and equipment deployed in their countries are reliable, safe, and secure. However, some markets — including **Brazil, China, India, Korea, Thailand, and Vietnam** — are using or proposing to use security concerns to justify *de facto* trade barriers. Requiring cloud service providers to confine data in-country does not improve security, but ultimately hinders it. 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 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. This 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 Korea**.

Customs Requirements on Electronic Transmissions: Across a broad cross-section of economic sectors that rely on the protection and enforcement of IPR, there are growing concerns about proposed domestic policies to improperly impose customs requirements on US digital exports — a development that would directly impact the United States' most innovative industries, including software and cloud computing services. Since 1998, World Trade Organization (WTO) Members have maintained a moratorium on customs duties on electronic transmissions. However, in 2018 **Indonesia** issued Regulation No.17/PMK.010/2018 (Regulation 17), which amends Indonesia's Harmonized Tariff Schedule to add Chapter 99: "[s]oftware and other digital products transmitted electronically."[4] These new tariff lines would cover many US digital exports — potentially everything from subscription services for music, film, and publications; to cloud and other remote software services; to data used in manufacturing plants; and a broad catch-all category of "other digital products." Other countries appear to be following Indonesia's path. Some countries, including **India** and South Africa, are working to

[4] 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."

undermine support for the WTO e-commerce moratorium[5] and push a work program at the World Customs Organization to impose customs requirements on electronic transmissions. If successful, these misguided efforts threaten to increase costs of digital products and services, and reduce productivity across sectors, in economies that would otherwise benefit from BSA members' software and technologies.

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 analytics systems are "trained" by ingesting large data sets to identify underlying patterns, relationships, and trends that are then transformed into mathematical models that can make predictions based on new data inputs. Following US leadership in this area, trading partners in East Asia, Southeast Asia, and Europe are taking a range of approaches to modernize their legal frameworks to permit the future development of, and international competition in, AI systems.

First, Japan enacted the Copyright Law Amendment Act ("the Act") in May 2018, which helps innovative US companies compete effectively in the Japanese market. Importantly, Article 30-4 of the Act permits both commercial and academic institutions to engage in data analytics, including through the creation of machine-readable copies that can be digitally analyzed and maintained for data validation purposes, provided that the user has lawful access to the data. Second, in January 2019, Singapore issued its Copyright Review Report, setting out its decision to amend the Copyright Act to (among other things) include a carefully calibrated framework permitting data analytics to be performed for both non-commercial and commercial purposes (subject to requirements of lawful access — e.g. via a paid subscription).[6] Third, 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. Thus, across four major legal systems, an emerging international legal consensus provides the business certainty necessary for the development of new AI-related products and services. BSA urges the US government to continue promoting such AI-focused legal frameworks, including in countries like **Brazil** — not only to foster innovation and creativity, but as a means of maintaining US technology leadership in AI and opening foreign markets to innovative US companies.[7]

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

---

[5] WTO submission by India and South Africa, "Moratorium on Customs Duties on Electronic Transmissions: Need For A Re-think ," July 12, 2018: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=247027,247023,246849,246824,246785,246786,246779,246780,246766,246733&CurrentCatalogueIdIndex=8&FullTextHash=

[6] 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

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

Patents: BSA members invest enormous resources to develop cutting-edge technologies and software-enabled solutions for businesses, governments, and consumers.[8] It is critical that countries provide effective patent protection to eligible computer-implemented inventions, in line with their international obligations. Some countries have adopted or are considering policies that could significantly constrain the freedom of patent holders to negotiate licenses for their inventions.

Software License Compliance: The use of unlicensed software by enterprises and governments is a major commercial challenge for BSA members. According to BSA's Global Software Survey — a global survey of more than 20,000 respondents that estimates the volume and value of unlicensed software installed on personal computers across more than 110 national and regional economies — the commercial value of unlicensed software globally is at least US$46 billion.[9] Not only does the use of unlicensed software impact the revenue stream of BSA members — deterring investments in further innovation, but it also exposes enterprises and agencies engaged in such activity to higher risks of malware infections and other security vulnerabilities.[10] Malware from unlicensed software costs companies worldwide nearly US$359 billion a year. Chief information officers (CIOs) report that avoiding data hacks and other security threats from malware is the number one reason for ensuring their networks are fully licensed.

Organizations now face a one-in-three chance of encountering malware when they obtain or install an unlicensed software package or buy a computer with unlicensed software on it — threatening economic loss of proprietary and sensitive data, trade secrets, and other important intellectual property. A single malware attack can cost a company US$2.4 million on average and can take up to 50 days to resolve. To the extent that the infection leads to company downtime, or lost business data, it can also seriously damage a company's brand and reputation. The cost for dealing with malware that is associated with unlicensed software is growing too. It can now cost a company more than US$10,000 per infected computer, and costs companies worldwide nearly US$359 billion a year.

BSA has engaged with US trading partners to reduce the incidence of unlicensed software use by enterprises and government entities, with varying degrees of success. These efforts include promoting 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, control, and protect their software assets and, as a result, ensure that all software is properly licensed. Governments can lead by example and adopt such measures for their own procurement and IT maintenance systems, which can send a powerful signal to enterprises in their countries.

Government and SOE Legalization: The use of unlicensed software by governments is particularly challenging to BSA members. Because BSA members rely on governments to provide protection and enforcement of their IPR, if governments are unwilling to comply with the law there is often little that BSA or our members can do on our own. We urge the US Government to use all available trade mechanisms, including Special 301, to engage with US trading partners on behalf of US companies on this important issue.

---

[8] 2018 Top 50 US Patent Assignees, *op. cit.* BSA members represented four of the top 10 US patent recipients in 2018, accounting for 47 percent of all US patents issued in 2018 to the top 10 recipients.

[9] 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

[10] *See id.*

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

Conclusion

BSA welcomes the opportunity to provide comments to inform the development of the 2020 Special 301 Report and the US Government's engagement with key trading partners. We look forward to working with USTR and the US agencies represented on the Special 301 Subcommittee of the Trade Policy Staff Committee to achieve meaningful progress on the issues described in this submission.

Table of Contents

Priority Watch List

CHILE

Due to continuing high levels of unlicensed software use by enterprises and its overdue implementation of FTA commitments, BSA recommends that Chile be maintained on the Priority Watch List.

Overview/Business Environment

The fundamental issue of concern for BSA members in Chile is the high rate of unlicensed use of software by enterprises and the absence of meaningful actions by the government to address the problem.

Copyright and Enforcement

The rate of unlicensed software in Chile has dropped only marginally from 57 percent in 2015 to 55 percent in 2017 (most recent available data). This represents a commercial value of US$283 million in unlicensed software.[11] Chile has not issued or changed any policies to specifically address unlicensed use of software since last year's report. Most service industry sectors, including architecture, design, engineering, and media continue to exhibit high rates of unlicensed software use. Problems also persist with the unauthorized pre-installation of software by hardware retailers, as well as in-house and external IT service providers that often load unauthorized copies of software onto computers or networks.

With respect to government legalization, the US-Chile FTA obligates the Government of Chile "to actively regulate the acquisition and management of software for … government use."[12] Although there has been some progress on government software legalization in Chile, further steps are necessary. Establishing and implementing appropriate provisions to regulate the acquisition and management of software by the government is critical to real success. The adoption of effective, transparent, and verifiable software asset management procedures — during which government agencies conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed — could also provide a positive example to private enterprises.

BSA's engagement with the main Chilean agency for intellectual property (IP), Instituto Nacional de Propiedad Industrial (INAPI) is productive. However, to improve the environment of IP protection and enforcement, BSA recommends that Chile prioritize the following three areas for legal reform:

- First, the US-Chile FTA contains detailed requirements for legal protections against the circumvention of technological protection measures used by BSA members to ensure that only licensed users are able to access their software products and services.[13] Chile has still not implemented necessary legislation and regulations to meet its obligations under this provision. As a result, in Chile it is easy to obtain illicit activation keys and services that offer the circumvention of technological protection measures.

- Second, damages awards remain too low to deter users of unlicensed software and there are no provisions for statutory damages. The FTA requires the availability of statutory damages.[14]

---

[11] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 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.

[12] United States – Chile Free Trade Agreement Article 17.7.4

[13] United States – Chile Free Trade Agreement Article 17.7.4.

[14] United States – Chile Free Trade Agreement Article 17.11.9.

- Third, in order to conduct civil inspections, civil *ex parte* actions remain a critical remedy for BSA. Unfortunately, these are hampered by a provision in Chilean law that requires filing *ex parte* search requests through a public electronic registry — allowing companies under investigation to learn about a search request before the inspection takes place. This notification requirement can significantly undermine the effectiveness of the search.

Recommendation

Due to continuing high levels of unlicensed software use by enterprises and the need for legal reforms consistent with Chile's FTA obligations, BSA recommends that Chile be maintained on the **Priority Watch List**.

CHINA

Due to a deteriorating market access environment for the software and IT sectors and continuing high levels of unlicensed software use by enterprises, BSA recommends that China be maintained on the Priority Watch List.

Overview/Business Environment

BSA members and other international technology providers face a particularly challenging commercial environment in China — both from a market access and intellectual property (IP) perspective.[15] 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. In its comments to the USTR in connection with the Administration's Section 301 investigation into China's trading practices, BSA highlighted several specific areas of concern: (a) foreign direct investment restrictions, including policies relating to Value-Added Telecommunications Services (VATS); (b) restrictions on cross-border data transfers; (c) requirements to disclose source code and enterprise standards; and (d) reliance on indigenous technical standards. BSA supports continued efforts by the US and Chinese governments to achieve mutually beneficial solutions to these challenges.

As regards intellectual property rights (IPR), we have seen encouraging progress on judicial enforcement. However, the commercial environment in China for software and information technology (IT) remains very challenging, especially with respect to policies and regulations that substantially hamper market access.

The Government of China has been building more effective judicial enforcement mechanisms for the protection of IPR by: implementing court procedures supporting evidence preservation; issuing guidance by the Supreme People's Court (SPC) on awarding higher damages for IP infringements; and establishing three new specialized IP courts in Beijing, Shanghai, and Guangzhou, as well as 10 IP tribunals in Suzhou, Nanjing, Wuhan, Chengdu, Hangzhou, Ningbo, Hefei, Fuzhou, Jinan, and Qingdao.

We continue to urge the Government of China to adopt effective, transparent, and verifiable software asset management (SAM) procedures. Such procedures would include having government agencies conduct audits of the software they have installed. This would help ensure that all copies in use by agencies are properly licensed and that relevant software is used efficiently and cost-effectively. By creating an inventory of software in use and reducing the instances of unauthorized or unlicensed software on government networks, implementing SAM will also help to reduce cybersecurity threats.

BSA is monitoring developments related to competition policy and the utilization of patents and other intellectual property (IP), and patent law reform. BSA urges meaningful reforms in the protection and enforcement of trade secrets in China, including how sensitive proprietary information that is required by government agencies for regulatory approval purposes is protected.

Regarding market access, China continues to present major challenges to BSA members. From 2017, the Government of China has issued numerous policies and standards designed to implement the Cybersecurity Law.[16] The law raises significant market access challenges relating to data localization,

---

[15] 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

[16] *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/

security, and privacy, which could be exacerbated or mitigated depending on how the implementing measures (many of which are still in draft form) are finalized. In addition, various government agencies have proposed sector-specific cybersecurity regulations that require firms to replace existing IT systems with “secure and controllable” products and services. The term “secure and controllable” is associated with vague requirements and is frequently interpreted by regulated entities as an instruction from the government to procure only domestic products and services.

Beyond cybersecurity, China’s regulatory regime also makes it extremely difficult for BSA members to participate in the digital market. China has proposed further restrictions to the existing system, which already effectively excludes foreign participation in cloud computing and other data services in China. While there have been some openings in the electronic commerce field and anticipated in some areas such as Multi-Party Communication Services (MPCS), China continues to regulate Internet and cloud computing services as value-added or basic telecommunications services (VATS or BTS) and precludes granting licenses to wholly owned or majority-owned foreign entities even for fundamental areas such as operating Internet Data Centers within China to serve the Chinese market.

These policies, combined with broader “indigenous innovation” policies, contribute to an increasingly challenging market access environment for many BSA members. In December 2018, China unveiled the latest draft of the proposed Foreign Investment Law, and in January 2020, China issued the final implementing regulations for the Foreign Investment Law. Some elements of those measures could result in a more level playing field, greater transparency in standards-setting processes, and better protections for investments (e.g. against state expropriation) and IPR.[17] Other provisions raise concerns, including a new and vaguely worded “security review system for foreign investment” (Art. 40); provisions that allow for expansion of the "negative list" of prohibited investments for purposes of “economic and social development” (Art. 4); and provisions that require only the publication of “normative” measures — whereas other measures need not be published (Art. 9). Furthermore, the vast majority of the concerns raised below are not addressed by the Foreign Investment Law revisions.

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

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

Cybersecurity Law: In November 2016, the National Peoples’ Congress passed the Cybersecurity Law (CSL), which went into effect in June 2017.[18] The law imposes a variety of obligations on “network providers”; imposes additional testing requirements on the procurement of certain software and services for “Critical Information Infrastructure” (CII) operators; limits international data transfers; and establishes a

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

[18] CSL, *op.cit.*

prescriptive personal data protection regime. Since early 2017, the Cyberspace Administration of China (CAC) and other authorities have been issuing measures and standards to implement the CSL. Many of these measures leave important issues vague and unclear (e.g., the definition of CII or "important information"), or appear to expand the scope of the law — exacerbating the negative impact of these rules on the software industry (e.g., requiring that all personal information and important information collected in China, and not just by CII operators, must be held in-country).

The expansive regulatory mandate advanced by the CSL has resulted in the emergence of numerous administrative initiatives to strengthen the government's role in managing networks, services, and data across nearly every sector of the Chinese economy. One prominent example of this is the Internet Security Supervision and Inspection Provisions by Public Security Organs released by the Ministry of Public Security (MPS) in September 2018, which codified and conferred broad authorizations for public security bodies to enforce the CSL.[19] This includes, among other things, the ability for public security bodies to conduct on-site and remote cybersecurity inspections on a broad (and indeterminate) range of companies that process and redistribute data or provide Internet services, and to impose a range of penalties (including fines and detention of individuals) for non-compliance.

Cybersecurity Classified Protection Regulation: On June 27, 2018, China established a de facto cybersecurity protection baseline for network operators and a universal compliance framework for the CSL by releasing the draft Cybersecurity Classified Protection Regulations (CCPR)[20] — a continuation of the Multi-level Protection Scheme (MLPS) jointly established by MPS, the State Encryption Management Bureau (SEMB), the Ministry of State Security (MSS), and the State Council Information Office (SCIO) in 2007.[21] Like MLPS, CCPR ranks the importance of network and information systems, based on their importance to China's national security, social order, public interests, and the legitimate interests of individuals and organizations, on a scale from 1 to 5, with Level 5 constituting the most sensitive to national security interests.

The draft CCPR also imposes several significant requirements regarding the structure and maintenance of networks operating within China. For instance, the draft CCPR requires that systems at Level 3 and above be connected with China's Public Security Bureau (PSB) system (managed by MPS) and that technical maintenance for such systems be performed within China. These unnecessarily intrusive requirements threaten to shut foreign technology out of systems ranked at CCPR Level 3 and above — constituting a significant point of concern for the industry at large.

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

A 1999 commercial encryption regulation deemed all commercial encryption products as "state secrets" and prohibited the use of foreign encryption products.[22] Unless companies can demonstrate that the 'core function' of the products they wish to sell is not encryption, then the product is banned from the Chinese market. Additionally, the State Commercial Cryptography Administration (OSCCA) requires

---

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

[20] *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

[21] *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

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

companies to turn over source code and other proprietary information for testing by state laboratories in order to gain market access for certain encryption products.

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

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

The Cybersecurity Law requires "personal information and other important data gathered or produced by critical information infrastructure operators during operations" to be stored within China.[24] In July 2017, the CAC issued draft Critical Information Infrastructure Protection regulations that contain an exceptionally broad definition of "critical information infrastructure" that would include cloud computing services.[25] These regulations, if enacted as drafted, would effectively require all cloud computing services providers (CSPs) operating in China to store data from their operations in China, thus creating additional operational costs and access challenges for foreign providers.

In June 2019, the CAC issued draft Security Assessment Measures for Cross-Border Transfers of Personal Information for public comment.[26] The draft measures require all cross-border transfers of personal information to undergo a security assessment by an appropriate local provincial-level cyberspace department, and prohibit the cross-border transfer of personal information where the transfer is "likely to impact national security or impair public interests." The draft measures — if adopted in their current form — create unacceptable legal risk and operational burden for CSPs dependent on cross-border data flows for their business operations and will serve as another key barrier to digital commerce.

Cloud Market Access: Cloud computing, despite being identified as an area of strategic development in China, remains largely off limits to foreign CSPs due to several policy challenges, including equity caps, investment restrictions, and connectivity requirements. These challenges are exacerbated by market entry barriers, such as restrictions on the ability to engage in cross-border data transfers and requirements to localize computing infrastructure.

---

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

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

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

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

In November 2016, the Ministry of Industry and Information Technology (MIIT) published a Draft Notice on Regulating Business Operation in Cloud Services Market (Draft Cloud Service Regulation Notice).[27] BSA and other associations submitted comments to the Government of China raising concerns about the Draft Cloud Service Regulation Notice and its implications for the operation of foreign cloud computing businesses in the country.[28]

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

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

Procurement: In May 2019, the CAC issued draft Cybersecurity Review Measures for public comment.[29] Under the measures, all “network products and services” purchased by critical information infrastructure operators will be subject to a cybersecurity review by the CAC. The measures do not define “critical information infrastructure” and could potentially require providers of products and services to provide access to valuable trade secrets and other IP, confidential commercial contract terms, and other sensitive information in order to pass the review. They also fail to specify what remedies are available for any wrong decisions made by the CAC. BSA and its members remain concerned that the measures and the review process will be used as a disguised market access barrier to foreign products and services.

There are also long-standing procurement measures in place, such as the MLPS.[30] The MLPS, and its proposed successor scheme the CCPS,[31] impose significant restrictions on the procurement of software and other information security products for an overly broad range of information systems the government considers sensitive. Among other requirements, procurement of such products is limited to those with IP owned in China. This applies to procurements by the government and increasingly to procurements by state-owned enterprises (SOEs) and the private sector, restricting market access for

---

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

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

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

[30] MLPS, *op. cit.*

[31] CCPS, *op. cit.*

foreign information security products. As a result, many entities in China are unable to procure the most effective software and security tools to meet their needs.

Foreign Direct Investment Restrictions: US businesses seeking to operate in China are subject to a range of foreign direct investment restrictions, including equity caps, and in-country hosting requirements, as well as challenging processes for obtaining licenses and other prerequisites for entering the market. These restrictions are particularly acute for the telecommunications and IT industries, including cloud computing services.

Under China's Telecommunications Service Catalog,[32] in conjunction with China's telecommunications regulations, China imposes a host of market access restrictions on foreign firms which are not typically regulated as telecommunications service providers in the rest of the world (e.g. data centers). The measures incorrectly classify a wide range of technologies and services as VATS or BTS, when in fact they are computer or business services that utilize the public telecommunications network as a method of delivery. For example, the catalog classifies cloud computing, content delivery networks, and online interactive platforms (called information services) as telecommunications services. Foreign firms that provide value-added services in China can only operate through joint ventures, of which they may own no more than 50 percent for VATS and 49 percent for BTS. In short, because of the update, foreign firms that provide a range of IT services are now subject to explicit limitations on market access, which also apply indirectly to local partners of joint ventures.

Intellectual Property

Intellectual Property and Competition: Prior to the establishment of the consolidated regulatory body — the State Administration for Market Regulation (SAMR) — several agencies under the State Council (i.e., the National Development and Reform Commission (NDRC), the State Administration of Industry and Commerce (SAIC), the Ministry of Commerce (MOFCOM), and the State Intellectual Property Office (SIPO)) were in the process of developing rules regarding the abuse, or misuse, of IP under the Anti-Monopoly Law (AML).[33] BSA members remain concerned that there may be divergent approaches to AML enforcement regarding IP — increasing business uncertainty, exposing rights holders to administrative abuse, and allowing agencies to use AML enforcement for industrial policy or other protectionist purposes. Specific concerns include applying rules tailored to standard-essential patents (SEPs) to non-essential patents not encumbered with voluntary "fair, reasonable, and non-discriminatory" (FRAND) licensing commitments. The US Government should continue to urge China to avoid using AML enforcement to undermine or prevent the normal and legitimate exercise of IP rights.

In November 2017, China passed a revised Anti-Unfair Competition Law (AUCL), which took effect on January 1, 2018.[34] BSA members are concerned about the broad definition of "unfair competition" in the AUCL and the overlap with the AML.

More recently, on March 29, 2018, the State Council released the Measures for Transfer of Intellectual Property Rights to Foreign Investors (Trial) with an aim to implement a holistic view of national security, improve China's national security system, and regulate the transfer of intellectual property rights to

---

[32] *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

[33] *Anti-Monopoly Law of the People's Republic of China,* August 2007 (Chinese), at: http://www.gov.cn/flfg/2007-08/30/content_732591.htm. English translation at: http://www.npc.gov.cn/englishnpc/Law/2009-02/20/content_1471587.htm

[34] *Anti-Unfair Competition Law of the People's Republic of China,* November 4, 2017 (Chinese) at: http://www.npc.gov.cn/npc/xinwen/2017-11/04/content_2031432.htm

foreign investors.[35] According to the Measures, matters subject to review include patents, integrated circuit layout designs, computer software copyrights, new plant varieties, and the right of application thereof. The review measures proposed by this legislation raise significant concerns for foreign investors surrounding IP protection and introduce considerable regulatory interference in commercial affairs.

In addition, technology companies are subject to insufficient and contradictory laws relating to contracts and liability for infringement. China's Contract Law generally permits contracting parties to negotiate on who will bear the liability for infringing products.[36] However, for technology import and export contracts, the Contract Law states that the position under the Technology Import and Export Regulations[37] will apply instead — requiring technology importers to indemnify their customers and bear the liability for infringing products. This lack of freedom to contract discriminates against overseas licensors and could be viewed as a non-tariff technical barrier.[38]

Source Code and Enterprise Standards Disclosure Requirements: Through a series of draft and final legislative documents, the Government of China has made clear its intention to establish a legal basis for requiring the disclosure of source code and enterprise standards (e.g. the specifications of an individual company's proprietary products or services) associated with foreign software products across a wide range of uses. Requirements to disclose source code and enterprise standards pose significant inherent risks to IP with little security value. It is critical that the Government of the United States intervene to eliminate current disclosure requirements and arrest further advancement of draft requirements.

The most significant measures relating to source code disclosure are found in the CSL, which includes requirements that products associated with CII be subject to security reviews.[39] Current implementing measures under the CSL contemplate that source code disclosures can be required as part of the security reviews but leave the specific mechanisms to future legislation.[40] The possibility of such mandated source code disclosures is cause for substantial concern among BSA members and other US companies. Additionally, as mentioned above in the area of cryptography, foreign commercial cryptography providers would be required to disclose source code to state licensers under the draft Cryptography Law.[41]

---

[35] *Measures for Transfer of Intellectual Property Rights to Foreign Investors (Trial)*, March 18, 2018 (Chinese), at: http://www.gov.cn/zhengce/content/2018-03/29/content_5278276.htm

[36] *Contract Law of the People's Republic of China*, March 15, 1999 (Chinese), at: http://www.npc.gov.cn/wxzl/gongbao/2000-12/06/content_5004732.htm. English translation at: http://www.npc.gov.cn/englishnpc/Law/2007-12/11/content_1383564.htm

[37] *Technology Import and Export Regulations of the People's Republic of China*, December 10, 2001 (Chinese), at: http://www.mofcom.gov.cn/article/swfg/swfgbf/201101/20110107353335.shtml. Unofficial English translation at: http://www.foreignercn.com/index.php?option=com_content&view=article&id=1181:regulations-on-technology-import-and-export-administration-of-the-peoples-republic-of-china&catid=55:chinese-law&Itemid=99

[38] The United States and the European Union have initiated WTO dispute settlement proceedings against China with respect to these Regulations and related measures. *See China – Certain Measures Concerning the Protection of Intellectual Property Rights,* Request for Consultations by the United States, WT/DS542/1 (March 26, 2018), copy at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/542-1.pdf; and *China – Certain Measures Affecting the Transfer of Technology,* Request for Consultations by the European Union, WT/DS549/1 (June 6, 2018), copy at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/549-1.pdf.

[39] CSL, *op. cit.*

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

[41] Draft Cryptography Law, *op. cit.*

Equally concerning are revisions to the Standardization Law enacted on November 4, 2017.[42] The revised law appears to require public disclosure of enterprise standards. Enterprise standards represent highly proprietary and confidential information that often is protected by trade secret law or other forms of IPR.[43] Their public disclosure would prove exceptionally damaging to the integrity of IP held by US technology companies.

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

Copyright and Enforcement

According to the latest information, the rate of unlicensed software use in China declined from 70 percent in 2015 to 66 percent in 2017. However, this rate remains extremely high, far above the regional (57 percent) and global (37 percent) rates. The estimated commercial value of unlicensed software in China was US$6.8 billion in 2017, the largest value by far among all US trading partners.[44]

Government and SOE Licensing/Legalization: BSA remains concerned that software legalization programs in China are not being implemented in a comprehensive manner. We urge the Government of China to implement comprehensive legalization programs for the government and SOEs that include: (1) audits, certification, and other credible processes to verify software license compliance; (2) software-asset management (SAM) best practices; (3) sufficient budgets to properly procure licensed legal software; (4) performance indicators to hold government and SOE officials accountable for ensuring measurable progress on software legalization; and (5) a prohibition on mandates or preferences for the procurement of domestic software brands as part of the legalization process.

Statutory and Regulatory Provisions: Draft amendments to the Copyright Act remain under review by the State Council Legislative Affairs Office. There is an urgent need for China to update and modernize its Copyright Law. BSA urges the Government of China to quickly enact copyright reform that:

- Clarifies that use of unlicensed software by enterprises is a violation of the reproduction right;
- Clarifies that unauthorized temporary reproductions, in whole or in part, are violations of the reproduction right (this will likely become increasingly important to BSA members as business

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

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

[44] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 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.

models shift to providing software in the cloud);
- Increases statutory damages, at least so that they are in line with the revised Trademark Act;
- Ensures that protections for technological protection measures (TPMs) extend to access controls, that the unauthorized sale of passwords and activation codes are explicitly defined as TPM circumvention, and that constructive knowledge of circumvention is sufficient to demonstrate a violation of the law; and
- Strengthens procedural provisions; for example, to explicitly grant courts more authority to compel evidence preservation and grant preliminary injunctions.

BSA notes that China's Criminal Law still does not address the widespread use of unlicensed software by enterprises in China.[45] While the Government of China amended the Criminal Law in 2015, the IP-related provisions of the Criminal Law (e.g., Articles 217 and 218 and other related provisions) were not updated. This represents an important missed opportunity to apply appropriate criminal remedies to copyright infringements which undermine the market and the incentives to bring to, or develop in, China cutting-edge software solutions. BSA continues to urge the Government of China to reconsider the decision not to amend the IP-related provisions of the Criminal Code. BSA urges China to impose criminal liability on enterprises that use unlicensed software, consistent with international best practices. BSA urges that the following issues be addressed and improved:

- Reduce thresholds that are too high (e.g., in the case of illegal income) or unclear (e.g., in the case of the copy threshold);
- Provide all commercial scale infringements with a criminal remedy. Because the requirement to show that the infringement is carried out "for the purpose of making profits" is not clear, law enforcement authorities have been reluctant to impose criminal liability on commercial enterprises using unlicensed software in the course of their business operations; and
- Define, distinct from copyright infringement, criminal violations for unauthorized circumvention of TPMs and trafficking in circumvention technologies, software, devices, components, and services, particularly the unauthorized sale of passwords or product activation codes or keys.

In addition to correcting the scope of criminal liability for IP violations, the Government of China should also amend the Criminal Code to lift the jurisdictional bar limiting foreign right holders from commencing a private civil claim against those being prosecuted for copyright crimes in local district courts, like Beijing and Jiangsu.

Compliance and Enforcement: The Government of China is building more effective judicial enforcement mechanisms for the protection of IP by establishing three specialized IP Courts in Beijing, Shanghai, and Guangzhou, as well as 21 IP tribunals in Suzhou, Nanjing, Wuhan, Chengdu, Hangzhou, Ningbo, Hefei, Fuzhou, Jinan, Qingdao, Shenzhen, Tianjin, Zhengzhou, Changsha, Xi'an, Nanchang, Lanzhou, Changchun, Wulumuqi, Haikou, and Xiamen. BSA and its members have had some success with the 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, several critical improvements are needed. 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

[45] *Criminal Law of the People's Republic of China*, July 1, 1979, incorporating the most recent 9th amendment in March 18, 2015 (Chinese), at: http://www.npc.gov.cn/npc/dbdhhy/12_3/2015-03/18/content_1930713.htm. Unofficial English translation at: https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china-2015

software. While some courts have increased damage awards based on SPC guidance, others, when facing similar infringement situations, grant much smaller statutory damages in lieu of a proper compensatory award. This problem highlights the need to increase statutory damages beyond those currently proposed in the draft amendments to the Copyright Act. Additionally, in cases in which a civil order is issued, right holders and authorities often face on-site resistance against evidence preservation and have only a limited amount of time to conduct software infringement inspections.

While the Criminal Case Transfer Regulations are well intentioned, they do not adequately address existing challenges to the effective transfer of administrative cases to criminal investigations and prosecution authorities.[46] Whether transfers are required upon reasonable suspicion that the criminal thresholds are met remains unclear under these regulations. Thus, 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.

Recommendation

Due to a deteriorating market access environment for the software and IT sectors and continuing high levels of unlicensed software use by enterprises, BSA recommends that China be maintained on the **Priority Watch List**.

[46] *Regulations on the Transfer of Suspected Criminal Cases by Administrative Law Enforcement Organs*, July 9, 2001 (Chinese), at: http://www.gov.cn/gongbao/content/2001/content_60972.htm

INDIA

BSA members continue to face challenges in providing products and services to the Indian market and experience persistently high rates of unlicensed software use by enterprises. For these reasons, BSA recommends that India remain on the Priority Watch List.

Overview/Business Environment

The commercial environment for BSA members remains challenging in India.[47] 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.

India has been working on a Personal Data Protection Bill since 2017. The most current version of the Bill — the Personal Data Protection Bill, 2019[48] — was introduced to the Indian Parliament in December 2019 and although changes have been 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 to what type of data would constitute critical or sensitive data are not provided), and a mandate that would potentially require data controllers to share non-personal data with the Central Government, among other issues.

In parallel to this important policy development, some sectoral regulators, including the Reserve Bank of India (RBI), have demonstrated support for data localization requirements. In February 2019, the Department for Promotion of Industry and Internal Trade (DPIIT) released a Draft National E-Commerce Policy, which mandated several proposals which would pose substantial challenges that would restrict the ability to provide customers in India with the most seamless and secure digital services. The draft policy included data localization 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.

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. Most recently, the Department of Industrial Policy and Promotion (DIPP) (now the DPIIT) issued the Public Procurement Order 2017 (Make in India Order), which requires government departments to give preference to local suppliers in procuring goods and services.[49] 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.

---

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

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

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

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,[50] to proposed regulations on personal data protection, regulations on machine-to-machine (M2M) systems,[51] and payment processing regulations.[52] These policies do not promote security.[53] Rather, they weaken data security and unfairly disadvantage firms that provide or rely on global cloud computing services.

There appear to be positive developments with respect to the patentability of software-related inventions. In July 2017, the Office of the Controller General of Patents, Designs, and Trade Marks (CGPDT) issued Revised Guidelines for Examination of Computer Related Inventions Guidelines (2017 CRI Guidelines).[54] The Guidelines removed the "novel hardware" requirement for patent eligibility in patent applications relating to computer-related inventions. This is encouraging as it is in line with international practice, as well as India's Patent Law, [55] and recognizes the possibility of software-enabled inventions receiving patent protection in India. It will be important to monitor how this revision is implemented in practice.

The use of unlicensed software by enterprises in India remains high. The most recent information indicates that the rate of unlicensed software use in India is 56 percent, representing a commercial value of unlicensed software of over US$2.5 billion.[56] This alarming figure highlights the scope of the problem and underscores the importance of pushing back against the use of unlicensed software by enterprises in India.

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 information technology (IT) sectors in general.

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

---

[50] 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

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

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

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

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

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

[56] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 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.

The Make in India Order,[57] issued by the DIPP in June 2017 to promote local manufacturing, requires every government department to give preference to local suppliers when procuring goods and services. The Make in India Order is the first enabling framework for preferential market access in software products and services. The order places an emphasis on the *situs* of manufacturing or provision of service (based on a definition of "local content"). However, government departments are granted the discretion to implement the Make in India Order according to their own requirements.

Subsequently, MeitY issued the Draft Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products in furtherance of the Order for public comment.[58] In July 2018, MeitY issued the final notification with only minor changes.[59]

In our written comments on the Draft Notification to MeitY, BSA raised several concerns.[60] For example, the "local supplier" requirements under the Notification represent unfair barriers to BSA members. The requirements include mandatory incorporation and registration in India, ownership of IP rights by the Indian entity (use, distribution, and modification), domestic revenue accrual from exploitation of such rights, and ambiguity with respect to computation of value addition, among other implementation challenges. Moreover, the scope of products and services enumerated in the notification is extremely wide and may be subsequently revised to include other types of software products and services.

The Notification and similar developments could significantly affect India's ability to acquire best-in-class products and services and negatively impact US companies' ability to effectively participate in public procurement opportunities.

***Data Sovereignty**:* On September 2019, MeitY constituted a Committee of Experts to develop a governance framework for non-personal data, or community data. It remains unclear exactly what kinds of data would constitute relevant non-personal, or community data, and exactly how such data might be regulated or for what purposes. However, this discussion has already had an indirect impact on the Personal Data Protection Bill 2019 (please see additional details below) which grants authority to the central government to require data fiduciaries and data processors 'to provide any non-personal data' to the government for unspecified purposes. These requirements in the PDP Bill 2019 could violate companies' intellectual property and other rights and have a chilling effect on innovation and investment in the digital economy. BSA supports the development of voluntary data sharing arrangements to facilitate data utilization and looks forward to contributing constructively to the Committee's discussions.

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

---

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

[58] *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

[59] *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

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

The Committee of Experts[61] (Expert Committee) on Data Protection under the Chairmanship of Justice B. N. Srikrishna (former Judge, Supreme Court of India) provides justifications for the introduction of data localization requirements in chapter six of the Report issued to MeitY in July 2018, while also recognizing that data localization may impose a substantial economic burden on companies. The Personal Data Protection Bill, submitted to MeitY by the Expert Committee, also contained problematic data localization requirements.[62] The 2018 Bill required that data fiduciaries store in India "at least one serving copy" of personal data subject to the Bill. BSA submitted formal comments on this measure in September 2018, raising our concerns with the data localization provisions, among other things, in detail.[63]

A revised version of the Bill was introduced to Parliament in December 2019 (PDP Bill 2019). Unfortunately, this version of the Bill continues to include seriously concerning provisions, including requirements to localize critical data (definition of what type of data would constitute critical data is not provided), to maintain copies of sensitive data in India (sensitive data definition 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 anonymised 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."

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.[64] 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.[65] 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.[66] The policy was subsequently withdrawn, and we expect that the DPIIT will issue a revised draft policy in 2020.

In 2015, the Department of Electronics and Information Technology (the predecessor to MeitY) issued a request for proposals for provisional accreditation of cloud service providers (CSPs) which mandated

---

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

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

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

[64] 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

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

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

"all services including data will have to reside in India."[67] 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.[68]

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."[69] 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.[70] The RBI provided payment firms a period of six months to comply with the Directive. This period elapsed on October 15, 2018, with the RBI refusing to extend the compliance deadline after repeated requests from industry. Although the RBI is not considering a suspension of services, it is exploring other actions to take against non-compliant firms. Furthermore, in early 2019, RBI notified banks that, according to its interpretation, the Directive applies to banks in addition to payment processors, which has been causing additional market access issues to US companies.

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: In July 2018, India issued the Personal Data Protection Bill prepared by the Expert Committee.[71] Although many aspects of the Bill would lay a strong foundation for a robust personal data protection framework if enacted, several requirements pose substantial challenges to BSA members and other organizations that operate globally. In comments submitted September 28, 2018, BSA voiced its concerns and recommendations to MeitY.[72]

In our comments, BSA describes our concerns that the Bill lacks the conceptual clarity and consistency that is crucial for the Indian digital economy to effectively integrate with the global data economy. In terms of regulatory capacity, although the Bill establishes an independent regulator called the Data Protection Authority, BSA is concerned this regulating body would not be properly resourced, would be asked to do too much, and may therefore prove ineffective. These challenges, coupled with serious concerns about data localization, adequacy requirements, disproportionate criminal penalties, lack of flexibility for personal data fiduciaries, uncertain accountability requirements, lack of an institutional framework for enforcement, nonflexible security safeguards, improper liability allocation, and lack of harmonization pertaining to the personal data of children, are broken down in greater detail in our comments.[73]

---

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

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

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

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

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

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

[73] *Ibid.*

Unfortunately, as stated in the previous sections of this submission, the version of the Bill submitted to the Indian Parliament in December 2019 (PDP Bill 2019) failed to address most of the concerns raised by BSA, 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 July 2018, a week before the Expert Committee published its Report and Draft Bill, the TRAI also submitted its recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector.[74] BSA had earlier submitted comments to the TRAI consultation process on privacy in October 2017, recommending that TRAI and other agencies of the Government of India work together and adopt clear and predictable stances on various issues relating to data protection.[75]

In December 2018, MeitY issued the Draft Information Technology [Intermediary Guidelines (Amendment) Rules] ("Draft Guidelines").[76] 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.[77] 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.[78] 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.[79] 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.[80] We are 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. Unfortunately, it is still unclear whether the TRAI is still considering potential server and data localization mandates.

---

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

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

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

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

[78] *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

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

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

Subsequently, the Department of Telecommunications released the National Digital Communications Policy — 2018 (NDCP 2018).[81] Notably, the NDCP 2018 highlights its mission to make "India a global hub for cloud computing and data communication systems and services" by "enabling a light touch regulation for the proliferation of cloud-based systems."

Intellectual Property

Patentability Guidelines for Computer-Related Inventions: The Computer-Related Inventions (CRI) Guidelines issued in 2017 by the Controller General of Patents, Designs, and Trademarks (CGPDT) — the product of several years of deliberation, stakeholder engagement, and study — represent an improvement from previous versions and provide some finality to a long public discussion on this issue.[82] Notably, the 2017 CRI Guidelines removed the "novel hardware" requirement for computer-related inventions. This is encouraging, as it is in line with international practice and recognizes the possibility of software-enabled inventions receiving patent protection in India. It will be important to continue monitoring how the revised guidelines are applied in practice.

Requirement to Report on Patent Working – Form 27: This Form 27 imposes India-unique reporting obligations on patent holders and licensees and does not create any benefits. The form creates an enormous compliance burden on patent holders and an enormous administrative burden on the Controller General of Patents, Designs & Trademarks, diverting resources from innovation on the one hand, and other more useful administrative functions (such as examining patent applications) on the other. It also exposes patent holders to the risk that sensitive information may be revealed and to legal liability for unintentional errors or incompleteness. And it is effectively impracticable for patent holders, especially in the software-related technologies and services industries, that manage enormous patent portfolios and whose products and services are composed of an enormous number of patents, both owned and licensed, that interact in complex ways, to comply with the requirement. BSA submitted comments to the Government of India in March 2018[83] and July 2019[84] urging the elimination of the form, or at least removal of some of the requirements it imposes, but to date, there has been no change to the form.

Compliance and Enforcement: The lack of statutory damages and inadequate damage awards in civil enforcement continues to be a challenge for BSA and our members when attempting to enforce our rights against enterprises using unlicensed software in India.

The *Commercial Courts, Commercial Division And Commercial Appellate Division Of High Courts Act 2015,* published on January 1, 2016, established commercial courts with jurisdiction over IP rights and related matters and limited the time the courts can take to decide cases.[85] Unfortunately, the potentially positive impact of the Ordinance was undermined by a Supreme Court judgement from July 2015, which requires software companies to file civil license infringement cases in district and high courts.[86] District and high courts have widely varying levels of experience and knowledge for handling such cases and there is uneven willingness to impose preliminary injunctions and important forms of preliminary relief. Furthermore, the system suffers from significant procedural delays.

---

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

[82] CRI Guidelines, *op. cit.*

[83] Comments available at https://www.bsa.org/files/policy-filings/03162018amendform27cgpdtm.pdf

[84] Comments available at https://www.bsa.org/files/policy-filings/06282019indiaamendform27dpiit.pdf

[85] *The Commercial Courts, Commercial Division And Commercial Appellate Division Of High Courts* available at: http://www.prsindia.org/sites/default/files/bill_files/Commercial_courts_Act%2C_2015_0.pdf

[86] Indian Supreme Court Judgement in IPRS v Sanjay Dalia & Anr., July 1, 2015

Criminal enforcement has also not proven to be practical for enforcing against enterprise use of unlicensed software. A draft report from an expert committee on cybercrime in October 2017 recommended the establishment of State Cyber Crime coordinators to improve India's criminal enforcement mechanisms.[87] However, even if a robust criminal enforcement system were established, an effective civil enforcement system will continue to be important for dealing with software license compliance-related issues.

Recommendation

BSA members continue to face challenges in providing products and services to the Indian market and experience persistently high rates of unlicensed software use by enterprises. For these reasons, BSA recommends that India remain on the **Priority Watch List.**

[87] *Set up cyber crime cells at district level: Expert panel* available at: https://timesofindia.indiatimes.com/india/set-up-cyber-crime-cells-at-district-level-expert-panel/articleshow/60876626.cms

INDONESIA

Due to a poor market access environment for the software and IT sector and rampant levels of unlicensed software use, BSA recommends that Indonesia remain on the Priority Watch List.

Overview/Business Environment

The commercial environment for the software and IT sector in Indonesia is very challenging.[88] 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. In addition, the use of unlicensed software by enterprises in Indonesia is among the highest in the region at 83 percent, representing a commercial value of unlicensed software of approximately US$1.1 billion — a situation that materially harms the legitimate software market in Indonesia and puts the enterprises using unlicensed software at risk for security vulnerabilities and malware.[89]

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."[90] 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 of 2019 on the Operation of Electronic Systems and Transactions (GR71) to supersede and replace GR82. GR71

---

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

[89] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 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.

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

explicitly clarifies that public sector data must be managed, stored, and processed in Indonesia, but that there is no similar restriction on private sector data, which can be managed, stored, and processed anywhere, subject to requirements with respect to financial sector data that may be imposed by the financial sector regulator. 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. While BSA welcomes GR71's recognition of the principle that private systems operators should be permitted to make their own determinations on optimal data storage locations, BSA is concerned about open-ended language in GR71 that appears to imply that specific Indonesian ministries may in the future choose to derogate from this principle in (as yet) undefined circumstances. The financial sector regulators (Bank Indonesia and OJK) have already indicated that they will continue to impose previous localization mandates with regards to private sector financial institutions that they regulate, regardless of the GR71 mandates that have otherwise called for alignment. 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).

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.

Local Content Regulation: In 2015, Kominfo published Regulation 27, which introduced local content requirements for 4G products — requiring such products imported into Indonesia to meet 20-40 percent local content (in terms of components, value-add, etc.). The Ministry of Industry published a corresponding regulation that stipulated how local content is to be computed and certified to the required percentage levels, including requirements for establishing local manufacturing facilities.

In 2019, Kominfo published a new regulation that extended this policy to cover all wavelength division multiplexing telecommunication tools and devices (Regulation 9 of 2019) and all Internet protocol network telecommunication tools and devices (Regulation 10 of 2019). The Ministry of Industry is now considering new regulations that would stipulate how local content would be computed for the broader scope of products covered by the 2019 regulations, which may include local content for software as well.

Indonesia's local content policies present a significant market access barrier for international companies and directly impact all ICT players in the market.

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

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 CBPRS, or according to standard contractual clauses, binding corporate rules, certifications, marks, or other approaches.

Over-the-Top Regulation: In mid-2016, Kominfo published a draft regulation (which was later updated in mid-2017) on the Provision of Application and/or Content Services Through the Internet.[91] This draft regulation threatens to impose unreasonable requirements on virtually all Internet-enabled services and service providers, including local physical presence and registration mandates, content filtering and censorship requirements, and mandatory use of local payment gateways, among others.

Intellectual Property

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

Copyright and Enforcement

According to the latest data, 83 percent of the software used in Indonesia is not licensed. This is one of the highest rates in the region and represents a commercial value of US$1.1 billion in unlicensed software.[92]

Recommendation

Due to a poor market access environment for the software and IT sectors, and rampant levels of unlicensed software use, BSA recommends that Indonesia remain on the **Priority Watch List**.

[91] *Draft Regulation on the Provision of Application and/or Content Services Through the Internet* (*Draft OTT Regulations)* (2016) (Indonesian) https://web.kominfo.go.id/sites/default/files/users/4761/Draft%20Uji%20PUblik%20Rancangan%20Permen%20Kominfo%20tentang%20Penyediaan%20Layanan%20Aplikasi.pdf

[92] 2018 BSA Global Software Survey, *op. cit.*

VIETNAM

Due to extremely high levels of unlicensed software use by enterprises and government institutions, the lack of criminal enforcement against use of unlicensed software by enterprises, and a number of increasingly troubling regulatory measures affecting market access for software products and services, BSA recommends that Vietnam be placed on the Priority Watch List.

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.[93] 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.[94]

BSA receives adequate support from the Ministry of Culture, Sports, and Tourism (MCST) and the High-Tech Crimes Department of the Public Security Ministry (High-Tech Police) in enforcing against the unauthorized use of software by enterprises in Vietnam. Unfortunately, the use of unlicensed software remains very high, both in the private and public sectors.[95]

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 implementing regulations suggest that the data localization and local presence requirements would only be implemented if a company fails to comply with a request under the Law from 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. BSA submitted comments on the proposed implementing regulations, aiming to minimize the negative impact of the law. However, it is not clear what, if any, due process or

---

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

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

[95] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 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.

judicial oversight may be available to companies that wish to contest an MPS order or penalties issued. Specifically, in respect to offshore service providers, the Government of Vietnam should request cooperation *in accordance with internationally recognized legal and diplomatic channels*, and introduce due-process mechanisms accordingly. The implementation decree should clearly state that organizations and companies that do not have visibility into or control the data being used to violate the laws will be excluded from the scope of Article 26.

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

Information Security: The National Assembly enacted the Law on Network Information Security (LONIS) on November 19, 2015. LONIS has been in force since July 1, 2016. BSA's concerns with the law and several implementing rules include obligations to disclose proprietary information as a condition to enter the market, overly broad definitions of personal information, and overly broad provisions requiring "cooperation with the Government" regarding access to data, which include requirements to decrypt encrypted information held by third parties. These provisions impact the ability of BSA members to provide services in Vietnam. It is also still unclear how the LONIS and the Cybersecurity Law will interact, raising additional uncertainty and compliance costs for BSA members.

In addition, Decree 58 of 2016, subsequently updated by Decree 53 of 2018, requires the Government Cipher Committee to issue licenses for products containing encryption. Considering the wide use of encryption in modern IT products to ensure confidentiality and integrity of information, the government's wide interpretation of products that require licensing has created a significant burden for international companies seeking to import IT products into Vietnam. We recommend that the scope of licensing be narrowed only to products that are specifically designed for protecting user information through the use of encryption, i.e. encryption should be the primary function of the product. If the encryption features can be turned off by the user or if it they are used for functions for the operation and management of the products, such licensing should not be required.

Cross-Border Data Flows and Server Localization: On September 1, 2013, Decree No. 72 went into effect. The decree imposes onerous server localization requirements and restrictions on cross-border data flows that will undermine the ability of BSA members to provide digital services. These measures may impact the ability of BSA members to provide software-based services online (e.g., cloud computing), which offer many economic benefits, especially to small and medium-sized enterprises in Vietnam.

Copyright and Enforcement

The rate of unlicensed software use is extremely high in Vietnam, far exceeding the global (37 percent) and regional (57 percent) averages. The latest data indicates that the rate of unlicensed software use in Vietnam is 74 percent, representing a commercial value of unlicensed software of US$492 million.[96]

Enterprise Licensing/Legalization: Enterprises in Vietnam, including foreign-invested enterprises, tend to place a very low priority on purchasing and using licensed software. Both the MCST and the High-Tech Police are supportive of BSA efforts to enforce against the unauthorized use of software by enterprises in Vietnam.

[96] 2018 BSA Global Software Survey, *op. cit.*

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code,[97] the Criminal Code,[98] and the Administrative Violations Decree.[99] The Civil Code operates in parallel.[100]

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.[101] 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: BSA significantly relies on administrative enforcement to combat the unlicensed use of software by enterprises in Vietnam. BSA is working in partnership with the Vietnam Copyright Office and the Inspectorate of the MCST to address the use of unlicensed software in Vietnam.

The Partnership in Protection of Software Copyright was established in 2008. Unfortunately, fines issued in administrative actions to date remain too low to constitute an effective deterrent against future infringements. Fines have been in the range of VND20-50 million (roughly US$1,000 – US$2,000), which is less than 10 percent the maximum applicable fine. The Government of Vietnam should use existing authorities, including the amendments to the Criminal Code (Article 225), to enhance the fines imposed on commercial infringers — greater fines can act as a strong deterrent against unlicensed software use.

---

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

[98] *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

[99] *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.

[100] *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

[101] *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

While BSA received good support from government agencies in 2018 for a National Crackdown Campaign, 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 has managed to bring only two cases to civil court since 2015. 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.

Recommendation: Due to extremely high levels of unlicensed software use by enterprises and government institutions, the lack of criminal enforcement against the use of unlicensed software by enterprises, and a number of increasingly troubling regulatory measures affecting market access for software products and services, BSA recommends that Vietnam be placed on the **Priority Watch List**.

Watch List

ARGENTINA

Due to continued challenges with high levels of unlicensed software use across the Argentine economy, BSA recommends that Argentina be placed on the Watch List.

Overview/Business Environment

Argentina has a poor track record of protecting and enforcing intellectual property rights relevant to cloud computing. Argentina has also not yet established a framework of "safe harbor" protections for intermediaries. Some gaps also exist in the important areas of standards development, as well as technology neutral and nondiscriminatory government procurement of information technology (IT).

Copyright and Enforcement

The rate of unlicensed software use across the Argentine economy is 67 percent, representing a commercial value of US$308 million in unlicensed software in 2017 (most recent available data).[102]

Argentina represents a challenging environment for copyright holders, as court processes are slow and complex, and penalties for copyright infringement are low. Argentina has high rates of copyright infringement, including online copyright infringement. BSA engages in civil actions in Argentina, with provisional injunctions representing a favorable feature of the civil system. In contrast, the criminal system is not an effective tool for enforcement, as IP enforcement is not a priority for prosecutors and effective remedies are not available. Similarly, IP enforcement is not a priority for customs authorities.

Argentina also faces a lack of enforcement against the act of circumvention, as well as the manufacturing or distribution of devices aimed at circumventing technological protection measures (TPMs), the absence of effective statutory damage provisions in civil infringement cases, and a failure to recognize IP ownership by legal entities on the same footing with natural persons. In addition, the availability of an intellectual property "safe harbor" for cloud service providers is limited and uncertain because there are no specific legislative provisions on this issue.

With respect to government legalization, the software industry continues to seek from the Argentine Government (the Subsecretaría de la Gestión Pública — the Under Secretariat for Public Administration) an executive decree that would mandate legal software use in government agencies. The decree should also require government agencies to implement verifiable software asset management (SAM) procedures when government agencies conduct audits of the software they have installed. This procedure would ensure, among other things, that all copies in use are properly licensed. While the Argentine Government has issued several guidelines on this issue, these have not been effective at addressing the continued use of unlicensed software in government agencies.

BSA recommends the following reforms to Argentine copyright law, including: (a) extending the scope of reproduction rights to explicitly cover temporary copies; (b) protecting against the act of circumvention, as well as the manufacture or distribution of devices aimed at circumventing technological protection measures (TPMs); (c) establishing effective statutory damage provisions in civil infringement cases; (d) establishing a statutory framework of "safe harbor" protections for intermediaries; and (e) recognizing

[102] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 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.

intellectual property (IP) ownership by legal entities on the same footing with natural persons to comport with international practice.

Recommendation: Due to continued challenges with high levels of unlicensed software use across the Argentine economy, BSA recommends that Argentina be placed on the **Watch List.**

BRAZIL

Due to a challenging market access environment for BSA members and continued high levels of unlicensed software use by enterprises, BSA recommends that Brazil remain on the Watch List.

Overview/Business Environment

Since President Bolsonaro took office in January 2019, the Brazilian and US governments have engaged in positive dialogues in various areas. For example, recent positive policy developments include the revocation of a decree that contained troublesome software auditing and source code disclosure requirements in the context of public procurement. In June 2019, Brazil issued guidelines on IoT that are also positive, although they have a broad scope of application. Furthermore, Brazil has recently launched public-private working groups to discuss the application of IoT on agriculture, on smart cities, on health 4.0 and industry 4.0 which should advance these discussions. The Government of Brazil is moving forward with the digitization of public services and is seeking to increase the use of digital tools by federal agencies and to create an environment that leverages emerging technologies, including artificial intelligence.

Even though Brazil has taken positive steps to improve market access recently, the overall market environment in Brazil remains challenging. We urge the US government to leverage the positive dialogues it has advanced with Brazil, including potential trade discussions to promote the elimination of current market barriers that impact US companies' ability to do business in Brazil.

Market Access

Current and pending legislation in the areas of data protection and public procurement of cloud services, as well as domestic procurement preferences have created, or threaten to create, *de facto* market access barriers for BSA members.

A variety of existing and proposed policies have created, or could create, *de facto* market access barriers for BSA members and may prevent them from providing the cutting-edge technologies and services increasingly demanded by Brazil's growing businesses. Concerns about privacy and security have been used to justify a variety of 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 in August 2018, and the law will come into force in August 2020. Legislation authorizing the creation of the Data Protection Agency (DPA) was approved in July 2019, but the DPA has yet to be fully established. DPA leadership appointments, other staffing decisions, as well as budget allocations are currently pending. The lack of a strong and properly funded DPA would have negative effects on the implementation of the Personal Data Protection Law and would impair cross-border data flows that are critical to market access for US companies selling goods and services in Brazil.

Data and Server Localization Requirements: The Guidelines on Government Procurement of Cloud Services were issued in late 2018 and include server and data localization requirements that will negatively impact the procurement of cloud computing services by all federal agencies. BSA submitted comments on the draft guidelines urging Brazil to remove the localization requirements. However,

Brazil did not adopt these recommendations, and the final Guidelines include the localization requirements.[103]

Government Procurement Preferences*:* Public procurement preferences for local products and services, as well as technologies developed in Brazil, are also required by the Guidelines on Government Procurement of Cloud Services, which was published in late 2018.

In addition, the Brazilian Congress is currently discussing potential changes to Brazil's Procurement Law. According to current law, the public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of IT systems can only be limited to local goods and services if such products and/or services are classified as "strategic" by a decree published by the government. A bill currently pending Congressional approval could remove the need for a decree classifying products and services as strategic. Although efforts to approve the bill are currently stalled, should the bill be approved in the future, any public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of IT systems could be limited exclusively to local goods and services, creating a market access barrier for foreign companies.

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 has announced it plans to issue a draft of the revised copyright law for public comment in early 2020.

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.[104] 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

---

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

[104] 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.

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.

As the software industry transitions to subscription-based software services and continues to devise other innovative ways to meet customers' changing demands for software (such as leveraging cloud computing and other Internet-enabled data services) the ability to enforce software licensing in the digital environment will continue to be key. BSA and its members look forward to working with the Brazilian Government to advance the enforcement of licenses in the digital environment.

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. Although the entity has the support of the Minister of Justice, the level of funding for the activities promoted by the agency is much lower than it used to be in past years. It is critical that the CNCP be properly funded, and that the agency continues to work closely with industry and vigorously expand its work beyond its traditional focus of counterfeiting and the piracy of physical goods.

Recommendation: Due to a challenging market access environment for BSA members and continued high levels of unlicensed software use by companies, BSA recommends that Brazil remain on the **Watch List**.

REPUBLIC OF KOREA

Due to a challenging market access environment for software products and services and a decrease in software license enforcement activities, BSA recommends that Korea be placed on the Watch List.

Overview/Business Environment

The overall commercial environment in the Republic of Korea (Korea) for BSA members and the software sector is mixed.[105] Korea has a strong IT market and a mature legal system. Over the past several years, however, the Government of Korea has adopted policies that have erected substantial market access barriers to foreign software products and services. Such policies include local testing requirements, and requirements to comply with national technical standards even when commonly used international standards are available. Although the Cloud Computing Promotion Act[106] 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.

The Government of Korea is actively developing its policies for moving Korea ahead in the digital economy. In 2017, the Administration established the Presidential Committee on the Fourth Industrial Revolution to formulate and implement a strategic plan for this purpose.[107] Government agencies have been reviewing regulations and considering regulatory reform or deregulation to stimulate innovation and growth in the digital economy. We urge the Government of Korea to use this opportunity to improve the overall business environment in Korea, especially for software and digital services.

Data suggests that the use of unlicensed software by enterprises is declining in Korea (see below).[108] Nevertheless, BSA remains concerned about persistent under-licensing of software in a variety of sectors and industries. This harms the legitimate commercial interests of BSA members and also raises potential security risks for the entities engaged in such activities. To continue combatting the use of unlicensed software by enterprises, the number of enforcement actions and investigations undertaken by the authorities each year should increase and the current system should be improved to create a more robust environment for copyright holders to take action against infringers. Such developments may include improving how evidence is obtained and exchanged in civil actions.

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

---

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

[106] *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

[107] See https://www.4th-ir.go.kr/home/en

[108] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 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.

members in 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 Korea's very broadly defined public sector. This is due to onerous certification requirements imposed by the Korea Internet Security Agency (KISA) 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 on-shoring apply to healthcare sectors.[109] Thus, even after enactment of the Cloud Computing Promotion Act, significant barriers to providing cloud computing and related services in Korea remain.

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

On July 23, 2019 the Ministry of the Interior and Safety (MOIS) and the Ministry of Science and ICT (MIST) announced revisions to Korea's Cloud Security Assurance Program (the Program).[110] The program requires 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." As described in BSA's August 2019 comments,[111] this requirement will have a negative impact on Korea's digital ecosystem and curtail its ability to participate effectively in the global digital economy — raising the cost of providing services and inhibiting the choice of technology available to end-users and procuring entities. The costs associated with such additional infrastructure will need to be recovered, which would ultimately increase the costs for end consumers.

The Regulation on Supervision of Electronic Financial Transactions (RSEFT)[112] was amended on October 5, 2016 to permit the use of cloud services by financial services institutions (FSIs). The amendment allows certain data to be stored on public cloud services. 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, FSC specifically requires that such data be maintained on servers located in Korea.[113]

---

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

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

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

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

[113] 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.

Encryption: The proposed revisions to Korea's Cloud Security Assurance Program (the Program) that MOIS and MIST announced in July 2019 requires that "cloud computing services providers shall use government-certified standard encryption technology when providing an encryption method for important material created through the cloud service." These kinds of national approaches to encryption, however, have limitations because of the global nature of the Internet, and the fact that criminal or terrorist acts are not limited by national borders. In fact, as outlined in BSA's comments, this kind of fragmented and piecemeal approach that only allows the use of domestically certified encryption standards may deprive organizations from using best-in-class encryption technologies, and this would weaken rather than strengthen the protection of sensitive data.[114]

Personal Information Protection Regime: Korea's personal information protection (PIP) regime is one of the most stringent in the region and has significantly decreased the ability for BSA members to serve the Korean market. Regulators and National Assembly members have been reviewing Korea's PIP regime, especially in light of negotiations with the European Commission on an "adequacy" recognition for Korea's personal information protection legal regime.

In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[115] the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act),[116] and the Credit Information and Protection Act.[117] 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 revised legislation is also expected to improve the ability to use certain kinds of data, especially pseudonymized and anonymized information, for commercial purposes. However, more work is required to reform Korea's personal data protection regime. Korea should 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.

In contrast to these recent more promising developments, the 2018 Network Act[118] requires global companies without local presence in Korea to designate a representative with information protection duties in Korea and limit onward transfers of personal information to third countries.

Domestic SME procurement in Public IT Network Equipment: MSIT enacted the Guideline of IT Network Equipment Installations in Public Sector (Guideline)[119] in 2017 to give preference to domestic small and medium-sized enterprises (SMEs). The Guideline significantly limits US suppliers' access to

---

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

[115] *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

[116] *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

[117] *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

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

[119] 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

many public sector procurement opportunities and may be inconsistent with Korea's international commitments. In 2018, MSIT proceeded to propose amendments to the Special Act on Promotion of Information and Communications Technology, Vitalization of Convergence Thereof, Etc. (ICT Special Act)[120] to provide a firmer legal basis for the Guideline. MSIT, in the explanatory note of the proposed legislative amendment,[121] stated that its intention is to raise the market share of domestic SME products in the public sector to a benchmark of over 96 percent (around 56 percent in 2017). This would match the share of SME products in the public sector software market in 2017.

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

Korea is a member of the Common Criteria Recognition Arrangement (CCRA) and therefore should recognize international certifications from accredited laboratories and should not impose further requirements for Common Criteria-certified products.[122] The additional requirements are not consistent with the spirit of CCRA, which is to "eliminate the burden of duplicating evaluation of IT products and protection profiles."[123] To make matters worse, a separate conformity test is required for each government agency, even for products procured and verified by another government agency.

This discriminatory application of security testing in public procurements to only international information security products also appears inconsistent with Korea's international commitments to national treatment and non-discrimination, including the US-Korea Free Trade Agreement (KORUS FTA). Although BSA and other organizations have raised this issue several times with the Government of Korea, the issue remains unresolved.

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

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

Copyright and Enforcement

The rate of unlicensed software use in Korea has continued a slow, steady decline. According to the latest available data, 32 percent of software used in Korea in 2017 was unlicensed, which equates to a

[120] 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

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

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

[123] *Ibid.*

market value of US$598 million in unlicensed software.[124] While this figure is below the regional and global average for unlicensed software use, there is still room for improvement. BSA acknowledges and supports the Government of Korea's goal to reduce the rate of unlicensed software use and efforts should be undertaken in pursuit of this objective.

To achieve this goal, the Government of Korea should lead by example by implementing and showcasing meaningful steps to reduce public sector use of unlicensed software; for example, by adopting effective software asset management (SAM) systems. This will set a positive example for the private sector and will also help address the serious cybersecurity risks that result from using unlicensed software. To facilitate this, BSA requests that the US Government open a dialogue with relevant representatives of the Government of Korea to identify mechanisms to address the issue of under-licensing of software across all sectors and industries.

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 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 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. Korea should amend the Civil Procedure Act, as the Supreme Court of Korea has suggested, to include effective discovery rules in civil cases.[125]

Recommendation

Due to a challenging market access environment for software products and services and a decrease in software license enforcement activities, BSA recommends that Korea be placed on the **Watch List**.

[124] 2018 BSA Global Software Survey, *op. cit.*

[125] *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

MEXICO

Due to the continued unlicensed use of software by enterprises, BSA recommends that Mexico remain on the Watch List.

Overview/Business Environment

The rate of unlicensed software use in Mexico has declined over the last several years, but unauthorized or counterfeit software remains available in most street markets. Concerns about unlicensed software use by enterprises and about judicial enforcement mechanisms are ongoing. The Government of Mexico should be commended for adopting software asset management (SAM) procedures in certain government agencies that comport with international best practices.

Copyright and Enforcement

A primary concern for BSA remains the unlicensed use of software by enterprises in Mexico. According to the most recently available data, the rate of unlicensed software in Mexico is 49 percent, representing an estimated commercial value of US$760 million in unlicensed software.[126] Illegal sales of software subscriptions, accounts, and usernames have become widespread and are commonly available at street markets ("carpeteros"), flea markets, and marketplaces, such as "Tepito," "Plaza Meave," "San Juan de Dios," "Pulgas" bazaars, and "Friky Plaza." Additional platforms for illegitimate sales include online auction sites, specialized file-sharing sites, and "white box" vendors — small local assemblers or off-brand vendors of computer hardware.

Ensuring that government agencies buy and use only legal software according to their licenses should be a priority. Mexico historically has been a global leader in terms of adopting transparent and verifiable SAM procedures in various government agencies, including the Mexican Tax Authority Administration (SAT) and the Mexican Institute of Industrial Property (IMPI). Consistent with new obligations in the United States-Mexico-Canada Agreement (USMCA), it is important that this trend continues.

While it is positive that IMPI precautionary measures have become increasingly effective, significant challenges to effective IP enforcement remain. Contrary to the Berne Convention, copyright certificates are still required in criminal cases in Mexico. Furthermore, a final ruling on a typical IP infringement case, brought to court after an administrative proceeding is concluded, is likely to take up to three to five years. Judicial procedures need to be streamlined to avoid excessive and unwarranted delays. A bill that would reform the Mexican Industrial Property Law, recently introduced in the Senate, would solve this issue, as well as the matter regarding the recovery of damages.

Consistent with the provisions of the USMCA, Mexico should move forward quickly to adopt and provide adequate legal protection and effective remedies against the circumvention of technical protection measures (TPMs) that control access to copyrighted works. These protections and legal remedies must apply to the act of circumventing TPMs, as well as the manufacturing, importation, distribution, offer for sale or rental, or provision of services that facilitate such circumvention. Although the Mexican criminal code punishes the domestic manufacturing of circumvention devices, the circumvention of TPM devices, components, "acts or services related to," importation, and trafficking in TPM tools have not yet been addressed by Mexican law.

---

[126] 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.

In addition, consistent with its USMCA commitments, Mexico should also ensure that adequate enforcement procedures and legal remedies are available for right holders to address copyright infringement online, i.e. effective injunctive relief. This should include implementing procedures, such as notice and takedown, to address allegations of infringement. As the Government of Mexico considers the legal changes in this area, it is important to ensure that the appropriate safe harbors be provided to Internet service providers (ISPs) and that such safe harbors are not conditioned on any obligation by the ISP to monitor or filter infringing activity. The Supreme Court's decision in the Amparo 1/2017 is still being used by ISPs as an argument to not fully cooperate with rights holders. ISPs, search engines, and OSPs continue to argue that there are more important rights than copyrights, such as the free access to the Internet, freedom of speech, privacy, and the like.

Further complicating criminal prosecutions are the requirements to produce expert opinions for every software infringement case, as well as physical copies of legal and illegal software. In many instances, these requirements cause premature termination of cases or undue delays. These requirements have a historic root, but they need to be changed drastically to adjust enforcement practices to current technology. The Mexican Attorney General's Office (PGR) continues to struggle with the transition from an inquisitorial to an adversarial criminal proceeding. The PGR's experts lack sufficient knowledge, training, and expertise to deal with digital copyright issues. PGR's Specialized Unit for the Investigation of Crimes Related to Copyright and Industrial Property Rights (UEIDDAPI) has recently suffered a considerable budgetary and staff reduction that negatively impact IPR enforcement actions. In addition, new unnecessary and bureaucratic requirements regarding the investigation of criminal conducts, the obtention of evidence by prosecutors, and the integration of criminal dockets, were introduced by UEIDDAPI in 2018 making the enforcement of IPR even more difficult in Mexico.

As evidenced through joint partnerships and corresponding activities, BSA's relationships with IMPI, INDAUTOR (the National Institute of Copyright), CONOCER (the National Council for Standardization and Certification of Labor Competences), CONALEP (the National College for Professional Technical Education), PGR, and the Cyber Police are positive.[127]

Recommendation: Due to the continued unlicensed use of software by enterprises, BSA recommends that Mexico remain on the **Watch List.**

[127] In 2018, BSA conducted training programs, and led or participated in a variety of round table discussions and other events that targeted a broad audience, including IMPI officers, officers from the Ministry of Education, the Ministry of Telecommunications, the Bank of Mexico, the National Banking and Securities Commission, and the Cyber Police, as well as customs inspectors, judges, industry association members, members of civil society, police officers, entrepreneurs, and students. The programs covered a broad range of IP issues, the importance of free flow of data, and other innovation-related topics. BSA carried out these activities in collaboration with various educational institutions, the Ministry of Education, the Ministry of Telecommunications, the Cyber Police, chambers of commerce, and associations. BSA also worked with think tanks including the Coalition for the Legal Access to Culture, and formalized alliances with the federal government by working with the Ministry of Education and the National Council for the Normalization and Certification of Working Competences (CONOCER).

THAILAND

Due to ongoing concerns regarding the level of unlicensed software use by enterprises in Thailand, as well as concerns about the implementation of security-related legislation now pending that may undermine the operations of BSA members, BSA recommends that Thailand remain on the Watch List.

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. 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.[128]

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

Market Access

BSA shares the goals of the RTG's Digital Economy initiative, Thailand 4.0, and supports the thoughtful 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.[129] There is also criminal liability for organizations and individuals who do not comply with executive orders issued under the Cybersecurity Act.

---

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

[129] 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

Personal Data Protection: The Personal Data Protection Act (PDP Act) was enacted in May 2019 (on the same date as the Cybersecurity Act) and is Thailand's first omnibus legislation on personal data protection. It is designed to build public trust and confidence in the digital economy and to implement the Asia-Pacific Economic Cooperation (APEC) Privacy Framework's principles for cross-border data transfers.[130] It also heavily draws from the General Data Protection Regulation (GDPR) of the European Union. BSA's chief concerns with the PDP Act relate to prescriptive and burdensome notification and consent requirements for the collection, use, and disclosure of personal data. There are also potentially challenging breach notification requirements and liability for personal data breaches imposed on data processors.[131]

Copyright and Enforcement

BSA enjoyed very good cooperation with RTG authorities in 2019, including with the Economic Crime Suppression Division (ECD) of the Royal Thai Police, in addressing unlicensed use of software in Thailand. The latest figures, however, indicate that the rate of unlicensed software use in Thailand was 66 percent in 2017, representing a commercial value of US$714 million.[132]

The rate of unlicensed software use in Thailand is well above the regional average of 57 percent across the Asia-Pacific — demonstrating that much greater efforts must be made. Beyond the use of unlicensed software by enterprises, the failure to fully implement the existing Cabinet resolution on legal software procurement, installation, and use in the public sector remains a problem for BSA members. The use of unlicensed software in the public sector may expose the RTG to unnecessary cybersecurity risks.[133] BSA urges the RTG to adopt software asset management (SAM) practices to eliminate the use of unlicensed software, strengthen enterprise risk management, and reduce cybersecurity risks.

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.

Government Engagement: BSA engaged with several RTG agencies to promote sound policies and legislation for the data driven economy in the context of the Thai Digital Economy initiatives, as well as to promote adequate IP protection and enforcement. The agencies BSA engaged with in 2019 included

---

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

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

[132] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 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.

[133] "*Unlicensed Software and Cybersecurity Threats*" available at: http://bsa.org/malware. *"Seizing Opportunity Through License Compliance"* report available at: http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. These reports demonstrate the link between unlicensed software and malware on personal computers (PCs).

the Department of Intellectual Property (DIP), the ECD, the Central Intellectual Property and International Trade Court (IP&IT Court), the Ministry of Digital Economy and Society (MDES), and the Digital Economy Promotion Agency (DEPA).

Technical Assistance and Education: In 2019, BSA, in collaboration with the DIP and the ECD, continued the joint national campaign to promote the use of licensed software. The campaign also explains the security risks posed by unlicensed software. BSA continued to promote SAM practices based on International Standards Organization (ISO) standards, reaching over 20,000 enterprises. BSA implemented campaigns to explain the benefits of SAM, including IT costs savings, reduction in cybersecurity and legal risks, and enhancement of corporate governance. Implementation of SAM practices would help reduce the use of illegal and unlicensed software in Thailand, bring about many benefits to the enterprises themselves, and benefit Thailand's economy in general.

Recommendation

Due to ongoing concerns regarding the level of unlicensed software use by enterprises in Thailand, as well as concerns about the implementation of cybersecurity and personal data protection legislation that may undermine the operations of BSA members, BSA recommends that Thailand remain on the **Watch List**.

Regions of Concern

EUROPEAN UNION

Continuing concerns regarding a growing number of measures that create market access barriers lead BSA to highlight the European Union as a Region of Concern.

Overview/Business Environment

Over the past five years, the European Union has modernized its digital economy regulatory and policy framework relevant to data service providers, in particular with regards to privacy, cybersecurity, data flows, and copyright. US data service providers expect this overhaul to continue under the new European Commission term which has recently started. They are confronted with growing rhetoric from the incoming EU leadership which aims to achieve EU's strategic autonomy and enhance its technological sovereignty. European authorities are considering measures that may constitute *de facto* market access barriers, including in the areas of data privacy, data sharing, artificial intelligence, and competition. While BSA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, some of these policies could limit the ability of US firms to offer digital services in the European Union. Moreover, there are legal challenges underway that could invalidate important existing mechanisms for transatlantic data transfers, such as the US-EU Privacy Shield and standard contractual clauses, adding further uncertainty for US data service providers.

Market Access

As the incoming European Commission develops and implements new policy proposals, BSA asks that the 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 focused on data transfers to the United States and have not applied the same scrutiny to data transfers relating to any other market, such as China, South Korea, or Russia.

In May 2016, the Irish Data Protection Commissioner requested that the Irish High Court ask the Court of Justice of the European Union ("CJEU") to examine whether Standard Contractual Clauses ("SCCs") violate EU citizens' fundamental rights insofar as there is insufficient judicial redress for EU citizens when their data is transferred to third countries, such as the United States. In May 2018, the Irish High Court finalized its Order for Reference to the CJEU, including 11 questions on the legality of the SCCs, the adequacy of the US legal system, and the legality of the Privacy Shield. In July 2018, the case and questions from the Irish High Court were docked at the CJEU, and BSA was officially accepted as amicus curiae at the CJEU. The Court held a public hearing on July 9th, 2019. The non-binding opinion of the Advocate-General was released on December 19, 2019 and a decision on the case is expected early 2020. While the Opinion recognizes that SCCs can provide adequate safeguards for international data transfers, the Advocate General identified a number of important shortcomings in the Privacy Shield, including with respect to private life and the right to an effective remedy, which, if supported by the Court, could lead to an invalidation of the Privacy Shield.

In parallel, the US-EU Privacy Shield, which replaced the former Safe Harbor framework for data transfers from Europe to the United States, took effect on August 1, 2016. The US-EU Privacy Shield represents a strong agreement to foster transatlantic data transfers, while safeguarding consumer privacy, as demonstrated by the number of companies certified to the program (over 4,900 in October 2019). Despite successful annual reviews (in 2017, 2018, and 2019), where the European Commission concluded that this framework continues to ensure adequate protection and safeguards for personal data transferred from the European Union to the United States, the Privacy Shield was immediately challenged before the EU General Court in cases brought by two privacy activist groups (Digital Rights Ireland and La Quadrature du Net). While the former has been dismissed, the latter has been admitted

but put on hold until the CJEU rules on its above-mentioned case regarding the validity of Standard Contractual Clauses as a transfer mechanism.

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

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

Dual-Use Export Controls Regulation: In September 2016, the European Commission published a Regulation aimed at revising the EU's regime for the control of exports and dual-use items. The draft legislation represents a deviation from the current international controls regime and could lead to tighter export controls, increased administrative burdens, and a potential risk for exporters of cybersecurity software products and services. Both the European Parliament and the Council have received their respective negotiating mandate, opening the way for trilogue negotiations to begin. The process is expected to conclude by summer 2020.

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.[134]

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

On February 15, 2019, in order to facilitate further discussion among the Council, the Romanian

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

Council Presidency published a revised text of the draft ePR. BSA continues to have serious concerns regarding the revised draft.[135]

In July 2019, BSA prepared an informal submission, answering the questions posed by the Finnish Presidency as preparatory work for the discussions in the Working Party on Telecommunications and Information Society on the ePrivacy Regulation.[136] As described at length in the submission, BSA highlighted the need to emphasize the importance of maintaining a clear distinction between the scope of the proposed ePrivacy Regulation and GDPR, and particularly the corresponding obligations they would establish. BSA also stressed the importance of ensuring the confidentiality of communications, the protection of personal data, and a clear distinction between personal and non-personal data. BSA also urged the Council to better align the ePrivacy Regulation with Art. 6 of the GDPR and to thoroughly analyze the scope of the regulation and its possible overlap with GDPR. The Finnish Presidency has published an updated text on October 4th 2019, addressing some of BSA's priorities. Nevertheless, BSA continues to voice its concerns, most recently by joining a cross-sector association letter, which called for the review of the whole proposal.

In December 2019, EU Member State Ambassadors rejected the ePrivacy Regulation compromise text presented by the Finnish Presidency, demanding more work on the file before it can be accepted by Member States and brought to Trilogue negotiations. Work is continuing under the Croatian Presidency and the European Commission is expected to assess how to progress with the file.

EU Cybersecurity Competence Centre: In September 2018, the European Commission published a draft Regulation on the establishment of the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The European Commission's proposal seeks to create an EU Cybersecurity Competence Centre aiming to ensure that Europe retains and develops essential cybersecurity technological capacities to protect critical networks and information systems, provide key cybersecurity services, and compete more effectively in the global cybersecurity market. If adopted as proposed, there is a risk that research funding and procurement decisions of the proposed Competence Centre may disadvantage some US-based companies, particularly in relation to: (1) provisions governing funding and procurement; and (2) industry's involvement in the work of the proposed Competence Centre.

Recommendation: Continuing concerns regarding a growing number of measures that create market access barriers lead BSA to highlight the European Union as a **Region of Concern.**

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

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