SPECIAL 301 SUBMISSION

February 7, 2019

Docket No. USTR-2018-0037

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

Dear Mr. Chang,

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 under Special 301 of the Trade Act of 1974 ("Special 301").[2]

Software has a profound impact on the American economy. The US software industry — and millions of American researchers, engineers, and other workers employed in this industry — benefit from American global leadership in the development and provision of software services, including cloud computing, data analytics, machine learning, cybersecurity solutions, and more. In 2016, the software industry was responsible for $1.14 trillion of total US value added GDP. The industry supported 2.9 million jobs (directly) and 10.5 million jobs (indirectly) — jobs that pay significantly higher than the national average for all occupations.[3] US exports of telecommunications, computer, and information services (including software) totaled more than US$42 billion in 2017. BSA members are among the top US patent recipients and annual US software research and development (R&D) investments total more than US$63 billion.[4] 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.

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

[2] Request for Comments and Notice of a Public Hearing Regarding the 2019 Special 301 Review, 83 Fed. Reg. 67468 (Dec. 28, 2018), available at: https://www.federalregister.gov/documents/2018/12/28/2018-28319/request-for-comments-and-notice-of-a-public-hearing-regarding-the-2019-special-301-review

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

[4] IFI Claims Patent Services, 2018 Top 50 US Patent Assignees (January 2, 2019) ("2018 Top 50 US Patent Assignees"), available at: https://www.ificlaims.com/rankings-top-50-2018.htm

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

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 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.

In this submission, we address both elements of Section 182 of the Trade Act.

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 — that have been critical drivers of US leadership in innovation and creativity, and US exports and job creation, in the digital economy. The ability of US companies to continue to lead global advances in innovative technology is under a rising threat from digital protectionism and isolationism, coercive technology transfer, and discrimination against foreign companies, products, and technologies. 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 data localization policies that restrict a company's ability to transfer data outside a country's territory where the data could be more effectively and securely stored or processed.

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

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, Mexico, South Korea, and Thailand
Regions of Concern:	European Union (EU)

Market Access and Intellectual Property Issues in Select Economies

To realize the economic promise of software, cloud computing, and emerging technologies, it is important to establish a legal framework that fosters innovation and promotes confidence in the digital economy. BSA's Cloud Scorecard examines the critical factors of such a legal framework, including in relation to IP, international trade, privacy, cybersecurity, voluntary standard-setting, and information technology (IT) readiness. Japan, Singapore, and the United States score well in this report due to their forward-looking trade, IP, and innovation policies (including their support for rules to permit data analytics). In contrast, China, India, Indonesia, Russia, and Vietnam receive the lowest rankings of all countries reviewed, due to policies that undermine not only investment in software innovation, but also market access for US IPR holders.

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

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

We highlight key market access and intellectual property issues below, exploring: (1) cross-border data flows and data localization; (2) security; (3) standards; (4) customs requirements on electronic transmissions; (5) artificial intelligence and machine learning; (6) Internet Service Provider (ISP) liability and safe harbors; (7) patents; (8) trade secrets and other proprietary information; (9) software license compliance; (10) government and state-owned enterprise (SOE) legalization; and (11) procurement restrictions.

Cross-Border Data Flows and Data Localization: The ability of US companies to continue leading global advances in innovative technology is under a rising threat from foreign government policies that hamper US business models and hinder the international movement of data. Data-related market access barriers take many forms. Sometimes they expressly require data to stay in-country or impose unreasonable conditions in order to send it abroad. In other cases, they require the use of domestic data centers or other equipment. Sometimes the barriers are based on privacy or security concerns, but too often the real motivation is protectionism, as the policy means chosen are often significantly more trade-restrictive than necessary to achieve any legitimate public policy goal. Immediate attention to these threats is urgently needed. Unfortunately, some markets, including **China, India, Indonesia, Nigeria, and Vietnam**, have adopted or have proposed rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory.

Among several Chinese measures that restrict the ability to transfer data across borders, the draft 2017 Critical Information Infrastructure Protection regulations would effectively require all cloud computing services providers (CSPs) to store data in-country.[6] India too has imposed data localization requirements, including through India's Directive on Storage of Payment System Data issued by the Reserve Bank of India in 2018, which imposes data and infrastructure localization requirements.[7] Likewise, Vietnam's 2018 Cybersecurity Law[8] and draft implementing regulations impose improper data localization requirements. Similarly, Nigeria's Guidelines for Nigerian Content Development in Information and Communications Technology contain stringent local content and sourcing requirements that apply to both government and private sector purchases. These guidelines raise significant market access concerns for companies offering software, information technology (IT), and data services overseas. BSA also continues to monitor the application of measures in the **EU** that 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, Taiwan, Thailand, and Vietnam** — are using or proposing to use security concerns to justify *de facto* trade barriers. For example, the Financial Supervisory Commission (FSC) in Taiwan announced that it is working on new legislative proposals to require all banks to store critical data locally for security reasons. Requiring cloud service providers to confine data in-country does not improve security, but ultimately hinders it — preventing data from being backed up in multiple locations. Ultimately, security is a function of the quality and effectiveness of the mechanisms and controls maintained to protect the data in question.

---

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

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

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

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

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

Customs Requirements on Electronic Transmissions: Across a broad cross-section of economic sectors 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."[9] These new tariff lines would cover many US digital exports — potentially everything from subscription services for music, film, and publications; to cloud and other remote software services; to data used in manufacturing plants; and a broad catch-all category of "other digital products." Other countries appear to be following Indonesia's path. Some countries are working to undermine support for the WTO e-commerce moratorium[10] 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

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

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

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

subscription).[11] Third, in the EU, similar legislation is also under consideration. Finally, in the United States, the "non-consumptive" reproductions that are necessary for the development of AI-related technologies are considered fair use. Thus, across four major legal systems, an emerging international legal consensus provides the business certainty necessary for the development of new AI-related products and services. BSA urges the US government to continue promoting such AI-focused legal frameworks — not only to foster innovation and creativity, but as a means of maintaining US technology leadership in AI and opening foreign markets to innovative US companies.[12]

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 **Mexico,** have yet to modernize their copyright frameworks to accommodate the needs of stakeholders in the digital environment.

Patents: BSA members invest enormous resources to develop cutting-edge technologies and software-enabled solutions for businesses, governments, and consumers.[13] 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. For example, **China** maintains a variety of policies that unfairly restrict the ability of patent holders to exercise their legitimate rights to enforce their patents or to negotiate mutually acceptable licensing terms.

Trade Secrets and Other Proprietary Information: BSA members rely on the ability to protect valuable trade secrets and other proprietary information to maintain their competitive position in the global marketplace. US trading partners that fail to implement and enforce strong rules to protect trade secrets against misappropriation or unauthorized disclosure put BSA members' business operations at risk and prevent them from having legal recourse when misappropriation or unauthorized disclosure occurs. Given the ease by which such information can be transmitted, this presents serious challenges not only in the country in question, but also globally. Countries with weak trade secret protection rules, or that have (or are proposing) policies requiring disclosure of sensitive information include **China, India, and Indonesia.** In addition, countries including **China, Indonesia, and Malaysia** have implemented or proposed policies, such as sector-specific outsourcing or IT risk management frameworks, that require source code review of technologies or services. For example, the central bank of Malaysia (Bank Negara Malaysia) is proposing to require financial institutions to conduct comprehensive source code reviews of critical IT systems, outlined in the draft Risk Management in Technology (RMiT) framework.[14]

---

[11] 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

[12] 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

[13] 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.

[14] See section 10.12, Bank Negara Malaysia Risk Management in Technology Exposure Draft, available at: http://www.bnm.gov.my/index.php?ch=57&pg=543&ac=726&bb=file

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

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.[15] 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.[16] 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.

Rates of unlicensed software use exceed 50 percent overall in the Asia Pacific (57%), Central and Eastern Europe (57%), Latin America (52%), and the Middle East and Africa (56%).[17] In this regard, selected regional economies with elevated rates of unlicensed software use include:

- China (66%), Indonesia (83%), Philippines (64%), Thailand (66%), and Vietnam (74%);
- Egypt (59%), Kenya (74%), and Nigeria (80%);
- Greece (61%), Romania (59%), Russia (62%), and Ukraine (80%); and
- Argentina (67%), Brazil (46%), Chile (55%), and Mexico (49%).

Notably, in Ukraine, the high rate of unlicensed software use exceeds the regional average by over 20 percent, with a 2017 commercial value of US$108 million.[18]

---

[15] 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

[16] *See id.*

[17] *See id.*

[18] In contrast with previous Special 301 submissions, BSA has streamlined 2019 comments to better reflect the key markets where BSA is most active and can offer the greatest insight. Countries BSA has listed in previous submissions, including Kazakhstan, Russia, Romania, and Taiwan for instance, continue to create ongoing market access challenges for the software and IT industry. For more information on these markets, please see BSA's 2018 Global Software Survey at: www.bsa.org/globalstudy

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

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. Government and SOE use of unlicensed software remains a major issue in markets including **China and India.**

Some governments, like **Mexico**, have taken commendable steps to establish mechanisms within government agencies to ensure only licensed software is purchased and used. Other governments have made commitments to ensure licensing compliance in government agencies and government-funded entities, including SOEs. **China** has made multiple commitments to the United State to ensure the legal use of software by government agencies and SOEs, however BSA remains concerned that software legalization programs are not being implemented in a comprehensive manner in **China**.

Procurement Restrictions: Governments are among the biggest consumers of software products and services, yet many are imposing significant restrictions on foreign suppliers' ability to serve public-sector customers. Not only do such policies eliminate potential sales for BSA members, but they also deny government purchasers the freedom to choose the best available products and services to meet their needs. US trading partners with existing or proposed restrictions on public procurement of foreign software products and services include **Brazil, China, India, Indonesia, Taiwan, and Vietnam.** For example, Taiwan restricts procurement of cloud computing services by requiring all government data to reside in-country with their procurement contract, awarding high scores to vendors with local datacenters — representing a barrier to companies that have servers outside Taiwan.

Conclusion

BSA welcomes the opportunity to provide comments to inform the development of the 2019 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.

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

Table of Contents

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

P 202-872-5500
W bsa.org

Priority Watch List

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

P 202-872-5500
W bsa.org

CHILE

Due to continuing high levels of unlicensed software use by enterprises and its overdue implementation of free trade agreement (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. This represents a commercial value of US$283 million in unlicensed software.[19] 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."[20] 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 enjoys a good relationship with the main Chilean agency for intellectual property (IP), Instituto Nacional de Propiedad Industrial (INAPI), and conducted almost 70 civil compliance inspections of a variety of enterprises on behalf of its members in 2018. 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.[21] Chile has still not implemented necessary legislation and regulations to meet its obligations under this provision. As a result, 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.[22]

[19] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at: 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.

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

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

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

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

- 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**.

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

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.[23] BSA members recognize the importance of resolving longstanding bilateral challenges with China and have seen first-hand the challenges and evolution of China's policies in the technology sector. BSA supports continued dialogue by the US and Chinese governments to work towards achieving mutually beneficial solutions to these challenges.

Regarding 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.[24]

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 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 terms of market access, China continues to present major challenges to BSA members. In 2017 and 2018, the Government of China issued numerous policies and standards designed to implement the Cybersecurity Law.[25] The law raises significant market access challenges related to data localization, security, and privacy, which could be exacerbated or mitigated depending on how the implementing measures (many of which are still in draft form) are finalized. In addition, various

[23] 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

[24] This submission does not address and is distinct from the Section 301 investigation. To view BSA's submission to USTR on the Section 301 investigation, see: www.bsa.org/~/media/Files/Policy/Trade/05112018BSACommentsChinaProductTariffList.pdf

[25] *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/

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

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 domestic products and services.

Beyond cybersecurity, China's regulatory regime also makes it extremely difficult for BSA members to participate in the digital market. China has proposed further restrictions to the existing system, which already effectively excludes foreign participation in cloud computing and other data services in China. While there have been some openings in the electronic commerce field, China continues to regulate Internet and cloud computing services as value-added or basic telecommunications services (VATS or BTS) and precludes granting licenses to wholly owned or majority-owned foreign entities.

These policies, combined with broader "indigenous innovation" policies, contribute to an increasingly challenging market access environment for many BSA members. In December 2018, China unveiled the latest draft of the proposed Foreign Investment Law, which contains commitments that appear to assure foreign investors of a more level playing field and better protections for investments (e.g. against state expropriation) and IPR.[26] However, it remains unclear how the draft Foreign Investment Law will be implemented, if adopted, and if the challenges and concerns raised in this submission will be addressed. BSA urges the 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.[27] The law imposes a variety of obligations on "network providers"; imposes additional testing requirements on the procurement of certain software and services for "Critical Information Infrastructure" (CII) operators; limits international data transfers; and establishes a prescriptive personal data protection regime. Since early 2017, the Cyberspace Administration of China (CAC) and other authorities have been issuing measures and standards to implement the CSL. Many of these measures leave important issues vague and unclear (e.g., the definition of CII or "important information"), or appear to expand the scope of the law — exacerbating the negative impact of these rules on the software industry (e.g., requiring that all personal information and important information collected in China, and not just by CII operators, must be held in-country).

The expansive regulatory mandate advanced by the CSL has resulted in the emergence of numerous administrative initiatives to strengthen the government's role in managing networks, services, and data across nearly every sector of the Chinese economy. One prominent example of this is the Internet Security Supervision and Inspection Provisions by Public Security Organs released by the Ministry of Public Security

[26] *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.

[27] CSL, *op.cit.*

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

(MPS) in September 2018, which codified and conferred broad authorizations for public security bodies to enforce the CSL.[28] 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 officially established a cybersecurity protection baseline for network operators and a universal compliance framework for the CSL by releasing the draft Cybersecurity Classified Protection Regulations (CCPR)[29] — 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.[30] 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 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.[31] Unless companies can demonstrate that the 'core function' of the products they wish to sell are not encryption, then the product is banned from the Chinese market. Additionally, the State Commercial Cryptography Administration (OSCCA) requires companies to turn over source code and other proprietary information for testing by state laboratories in order to gain market access for certain encryption products.

More recently, in April 2017, SCA published a draft Encryption Law for public comment.[32] BSA is concerned with the draft law for several reasons. First, it would fully or partially bar foreign competition in various categories of cryptography. Of the three categories defined by the law (core, common, and

[28] *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

[29] *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

[30] *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

[31] *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

[32] *Encryption Law of the People's Republic of China (Draft for Comment)*, April 28, 2017 (Draft Encryption Law) (Chinese) at: http://www.oscca.gov.cn/sca/hdjl/2017-04/28/content_1011759.shtml. Unofficial English translation at: https://chinacopyrightandmedia.wordpress.com/2017/04/13/encryption-law-of-the-peoples-republic-of-china-opinion-seeking-draft/

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

commercial cryptography), foreign businesses would only be allowed to participate in the commercial cryptography market, and even then, only under strict regulations. Additionally, the draft law lacks a clear definition of the scope of commercial cryptography — leaving significant uncertainty about which products and services foreign companies might provide. And finally, the licensing scheme for foreign commercial cryptography providers, as envisioned by the draft law, would require such providers to disclose source code to state licensers, putting their IP at significant risk.

Cyber Critical Equipment and Cybersecurity Specific Product Catalog: The Catalog of Network (Cyber) Critical Equipment and Cybersecurity-Specific Products (Batch 1) was jointly released by CAC, the Ministry of Industry and Information Technology (MIIT), MPS, and the Certification and Accreditation Administration (CNCA) on June 9, 2017 with retroactive effect from June 1, 2017.[33] This was done without a comment period or consultation with industry. The Catalogue introduces a market-entry requirement for the equipment and products in the catalog, mandating they be certified or tested in accordance with relevant national standards before entering the market. It also introduces Chinese standards and "other mandatory requirements" which remain unspecified at this time. It is not clear whether such requirements will be aligned with applicable internationally recognized standards and be consistent with the World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT Agreement) obligation that technical regulations follow international standards where such standards exist.

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

The Cybersecurity Law requires "personal information and other important data gathered or produced by critical information infrastructure operators during operations" to be stored within China.[34] 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.[35] These regulations, if enacted as drafted, would effectively require all cloud computing services providers (CSPs) operating in China to store data from their operations in China, thus creating additional operational costs and access challenges for foreign providers.

In April 2017, the CAC issued draft Security Assessment Measures for Cross-Border Transfers of Personal Information and Important Data for public comment.[36] The draft measures contain obligations relating to security assessments, impose additional localization requirements and restrictions on the transfer of "personal information" and "important data" across borders, and restrict remote access to such data stored in China from outside its borders. The draft measures — if adopted in their current form — create unacceptable legal risk for CSPs dependent on cross-border data flows for their business operations and will serve as another key barrier to digital commerce.

Cloud Market Access: Cloud computing, despite being identified as an area of strategic development in China, remains largely off limits to foreign CSPs due to several policy challenges, including equity

[33] *Catalog of Network (Cyber) Critical Equipment and Cybersecurity-Specific Products (Batch 1)*, June 9, 2017 (Chinese), at: http://www.cac.gov.cn/2017-06/09/c_1121113591.htm

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

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

[36] *Security Assessment Measures for Cross-Border Transfers of Personal Information and Important Data (Draft for Comment)*, April 11, 2017 (Chinese) at: http://www.cac.gov.cn/2017-04/11/c_1120785691.htm

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

caps, investment restrictions, and connectivity requirements. These challenges are exacerbated by market entry barriers, such as restrictions on the ability to engage in cross-border data transfer and requirements to localize computing infrastructure.

In November 2016, MIIT published a Draft Notice on Regulating Business Operation in Cloud Services Market (Draft Cloud Service Regulation Notice).[37] 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.[38]

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 2017, the CAC issued the Interim Measures for the Security Review of Network Products and Services.[39] Under the measures, all "important network products and services" purchased for national security-related networks and information systems will be subject to review by third-party assessors operating under the auspices of a cybersecurity review office, to be established by the government. The measures do not define "important network products and services" or delineate what systems are national security related. They also fail to specify how the third-party assessors will be designated, the steps that an applicant should follow to have products or services reviewed, and what remedies are available for any wrong decisions made by the cybersecurity review office. BSA and its members remain concerned that the measures and the review process will be used as a disguised market access barrier to foreign products and services.

There are also long-standing procurement measures in place, such as the MLPS.[40] The MLPS, and its proposed successor scheme the CCPS,[41] impose significant restrictions on the procurement of software

[37] *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

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

[39] *Measures for the Security Review of Network Products and Services (Interim),* May 2, 2017 (Chinese) at: http://www.cac.gov.cn/2017-05/02/c_1120904567.htm. Unofficial English translation at: https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/

[40] MLPS, *op. cit.*

[41] CCPS, *op. cit.*

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

and other information security products for an overly broad range of information systems the government considers sensitive. Among other requirements, procurement of such products are limited to those with IP owned in China. This applies to procurements by the government and increasingly to procurements by state-owned enterprises (SOEs) and the private sector, restricting market access for foreign information security products. As a result, many entities in China are unable to procure the most effective software and security tools to meet their needs.

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

In March 2016, a new Telecommunications Service Catalog went into effect, expanding the scope of China's telecommunications regulations and imposing a host of associated market access restrictions on foreign firms which are not typically regulated as telecommunications service providers (TSPs) in the rest of the world.[42] The measures incorrectly classify a wide range of technologies and services as VATS or BTS, when in fact they are computer or business services that utilize the public telecommunications network as a method of delivery. For example, the catalog classifies cloud computing, content delivery networks, and online interactive platforms (called information services) as telecommunications services. Foreign firms that provide value-added services in China can only operate through joint ventures, of which they may own no more than 50 percent for VATS and 49 percent for BTS. In short, because of the update, foreign firms that provide a range of IT services are now subject to explicit limitations on market access, which also apply indirectly the local partners of joint ventures.

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).[43] 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.[44] BSA members are concerned about the broad definition of "unfair competition" in the AUCL and the overlap with the AML.

---

[42] *Classification Catalogue of Telecommunications Services (2015 Edition)*, December 28, 2015 (Chinese), at: http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c4564595/content.html

[43] *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

[44] *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

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

More recently, on March 29, 2018, the State Council released the Measures for Transfer of Intellectual Property Rights to Foreign Investors (Trial) with an aim to implement a holistic view of national security, improve China's national security system, and regulate the transfer of intellectual property rights to foreign investors.[45] 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.[46] However, for technology import and export contracts, the Contract Law states that the position under the Technology Import and Export Regulations will apply instead — requiring technology importers to indemnify their customers and bear the liability for infringing products.[47] This lack of freedom to contract discriminates against overseas licensors and could be viewed as a non-tariff technical barrier.[48]

Source Code and Enterprise Standards Disclosure Requirements: Through a series of draft and final legislative documents, the Government of China has made clear its intention to establish a legal basis for requiring the disclosure of source code and enterprise standards (e.g. an individual company's proprietary product or services specifications) associated with foreign software products across a wide range of uses. Requirements to disclose source code and enterprise standards pose significant inherent risks to IP with little security value. It is critical that the US Government 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.[49] 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.[50] The possibility of such mandated source code disclosures is cause for substantial concern among BSA members and other US companies. Additionally, as mentioned above in the area of cryptography, foreign commercial cryptography providers would be required to disclose source code to state licensers under the SCA's draft Encryption Law.[51]

---

[45] *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

[46] *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

[47] *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

[48] 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

[49] CSL, *op. cit.*

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

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

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

Equally concerning are revisions to the Standardization Law enacted on November 4, 2017.[52] 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.[53] Their public disclosure would prove exceptionally damaging to the integrity of IP held by US technology companies.

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

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.[54]

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 itself 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

[52] *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

[53] 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.

[54] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at: 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.

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

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.[55] 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 10 IP tribunals in Suzhou, Nanjing, Wuhan, Chengdu, Hangzhou, Ningbo, Hefei, Fuzhou, Jinan, and Qingdao. BSA and its members have had some success with the IP Courts and tribunals.[56] 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 software. While

[55] *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

[56] For example, Adobe & Autodesk vs. Beijing Ourpalm Technology Co.; Adobe & Autodesk vs Shanghai Fengyuzhu Exhibition Co.; Dessault & Autodesk vs. Zhongshan Xinhai Precision Manufacture.

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

some courts have increased damages 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.[57] 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 remain on the **Priority Watch List**.

[57] *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

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

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

The Committee of Experts[59] (Expert Committee) on Data Protection under the Chairmanship of Justice B. N. Srikrishna (former Judge, Supreme Court of India) submitted its Data Protection Committee Report (Report)[60] and the Personal Data Protection Bill, 2018 ('Bill')[61] to the Ministry of Electronics and IT (MeitY) in July 2018. This Bill has seen extensive debate, as it includes contentious provisions such as localization requirements for personal data and restrictions on the cross-border transfer of personal data. In parallel to this important policy development, some sectoral regulators, including the Reserve Bank of India (RBI), have demonstrated support for data localization requirements.

Government procurement policies remain outmoded and inefficient because of local content and technology preferences. Most recently, the Department of Industrial Policy and Promotion (DIPP) issued the Public Procurement Order 2017 (Make in India Order), which requires government departments to give preference to local suppliers in procuring goods and services.[62] In addition, the Draft National Policy on Software Products would promote the use of domestically developed software products in public sector procurements and strategic sectors like defense, telecommunications, energy, and healthcare. Such policies do not offer a level playing field to US technology providers that are bringing cutting-edge technologies and services to India.

The existing and future software market in India remains at risk due to a variety of existing or proposed data localization requirements. From legacy policies on government-owned weather data,[63] to proposals

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

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

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

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

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

[63] 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

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

regarding machine-to-machine (M2M) systems,[64] payment processing,[65] and existing public procurement requirements like the Make in India Order,[66] the Government of India appears to be considering requiring the localization of data sets within India for a variety of reasons. These policies do not promote security.[67] 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).[68] The Guidelines removed the "novel hardware" requirement for patent eligibility in patent applications relating to computer-related inventions. This is encouraging as it is in line with international practice, as well as India's Patent Law, and recognizes the possibility of software-enabled inventions receiving patent protection in India. It will be important to monitor how this revision is implemented in practice.[69]

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.[70] 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 affecting the commercial environment for BSA members and the software and information technology (IT) sectors in general.

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

The Make in India Order,[71] 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.

---

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

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

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

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

[68] *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

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

[70] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at: 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.

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

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

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.[72] In July 2018, MeitY issued the final notification with only minor changes.[73]

In our written comments on the Draft Notification to MeitY, BSA raised several concerns.[74] For example, the "local supplier" requirements under the Notification represent unfair barriers to BSA members. The requirements include mandatory incorporation and registration in India, ownership of IP rights by the Indian entity (use, distribution, and modification), domestic revenue accrual from exploitation of such rights, and ambiguity with respect to computation of value addition, among other implementation challenges. Moreover, the scope of products and services enumerated in the notification is extremely wide and may be subsequently revised to include other types of software products and services.

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

Data Localization: There are a variety of examples where the Government of India has imposed, or proposes to impose, data localization requirements. In 2015, the Department of Electronics and Information Technology (the predecessor to MeitY) issued a request for proposals for provisional accreditation of cloud service providers (CSPs) which mandated "all services including data will have to reside in India."[75] 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.[76]

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."[77] Additionally, "data" is defined very broadly, and the Directive is likely to affect not only the payment processors, but also companies providing services to payment processors. BSA submitted comments to the RBI June 22,

---

[72] *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

[73] *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

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

[75] 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

[76] 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

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

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

2018, voicing concern about these data localization requirements.[78] 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.

The Expert Committee on Data Protection provides justifications for the introduction of data localization requirements in chapter six of the Report issued to MeitY in July 2018, while also recognizing that data localization may impose a substantial economic burden on companies.[79] The Personal Data Protection Bill, submitted to MeitY by the Expert Committee at the same time, also contains problematic data localization requirements.[80] The Bill requires that data fiduciaries store in India "at least one serving copy" of personal data subject to the Bill. BSA submitted formal comments on this measure in September 2018, raising our concerns with the data localization provisions, among other things, in detail.[81]

One more example of how the Government of India seems to be aggressively promoting the concept of data localization is in the cloud computing policy environment. MeitY established the Working Group on Cloud Computing (Working Group) to look into policy issues concerning cross-border data flow and data security. Unfortunately, recent reports indicate that the Working Group may include broad data localization requirements for CSPs providing services both to the public and private sectors in its recommendations to MeitY.[82]

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

Cloud Computing: In June 2016, the Telecom Regulatory Authority of India (TRAI) released a consultation paper requesting stakeholder input on a range of important questions regarding cloud computing.[83] 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.[84] 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.

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

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

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

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

[82] 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

[83] *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

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

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

The TRAI then released its recommendations in August 2017.[85] It is encouraging that the TRAI recommended a "light touch" approach to cloud computing regulation and emphasized the need for flexibility and choice by way of contractual agreements between CSPs and end-users. Unfortunately, it is unclear whether the TRAI is still considering potential server and data localization mandates.

The Department of Telecommunications released the National Digital Communications Policy — 2018 (NDCP 2018).[86] Notably, the NDCP highlights its mission to make "India a global hub for cloud computing and data communication systems and services" by "enabling a light touch regulation for the proliferation of cloud-based systems."

Privacy and Personal Data Protection: In July 2018, India issued the Personal Data Protection Bill prepared by the Expert Committee.[87] 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.[88] Since then, MeitY has been examining submissions from hundreds of stakeholders with the aim of tabling a version of the Bill with the aim of tabling legislation to the Parliament after 2019 general elections.

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.[89]

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.[90] 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.[91]

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

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

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

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

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

[89] *Ibid.*

[90] *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

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

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

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.[92] Notably, the 2017 CRI Guidelines removed the "novel hardware" requirement for computer-related inventions. This is encouraging, as it is in line with international practice and recognizes the possibility of software-enabled inventions receiving patent protection in India. It will be important to monitor how the revised guidelines are applied in practice.

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.[93] 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.[94] 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.

Criminal enforcement has also not proven to be practical for enforcing against enterprise use of unlicensed software. A recent 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.[95] 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.**

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

[93] *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

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

[95] *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

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

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.[96] A variety of authorities have issued, or are in the process of developing, policies that will raise the cost of providing digital products or services to the Indonesian market. 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.[97]

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."[98] 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 on the Operation of Electronic System and Transaction (GR82) in October 2012.[99] The Indonesian Ministry of Communication and Informatics (Kominfo) subsequently issued two implementing regulations under GR82: (1) Regulation No. 36 of 2014 on the Registration Procedure for Electronic System Operators;[100] and (2) Regulation No. 20 of 2016 on the Protection of Personal Data in

---

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

[97] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at: 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.

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

[99] *Government Regulation No. 82* (2012) (Indonesian) at: http://www.flevin.com/id/lgso/translations/JICA%20Mirror/indonesia/4902_PP_82_2012_i.html. Unofficial English Translation at: http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html

[100] *Kominfo Regulation No. 36 on the Registration Procedure for Electronic System Operators* (2014) (Indonesian) at: https://jdih.kominfo.go.id/produk_hukum/unduh/id/235/t/peraturan+menteri+komunikasi+dan+informatika+nomor+36+tahun+2014+tanggal+30+september+2014

Electronic Systems (Electronic Data Protection Regulation).[101] These regulations raise concerns regarding data and IT infrastructure localization mandates, unreasonable obligations on data service providers, and other matters. Such requirements will increase costs, harm the quality of data services, and interfere with the assurance of data security without enhancing information security or protection.

On February 1, 2018, Kominfo shared a Draft Amendment to amend GR82. BSA, along with several other trade associations, submitted comments to Kominfo, discussing the potentially problematic provisions within the text and calling for further clarification.[102] BSA's chief concerns focus on:

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

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

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

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.[103] This draft regulation threatens to impose unreasonable requirements on virtually all Internet-enabled services and service providers, including local physical presence and registration mandates, content filtering and censorship requirements, and mandatory use of local payment gateways, among others.

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

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

Copyright and Enforcement

According to the latest data, 83 percent of the software used in Indonesia is not licensed. This is one of the

[101] *Kominfo Regulation No. 20 on the Protection of Personal Data in Electronic Systems (Electronic Data Protection Regulation)* (2016) (Indonesian) at: https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016

[102] Joint Industry Comments on Draft Amendments to GR82 (March 1, 2018) available at: https://www.bsa.org/~/media/Files/Policy/Data/03012018BSAJointSubmissionOnGR82Amendment.pdf

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

highest rates in the region and represents a commercial value of US$1.1 billion in unlicensed software.[104]

Statutory and Regulatory Provisions: Indonesia enacted a new copyright law in 2014.[105] The law clarifies that software is copyrightable and that "compilations of creations or data in a format that can be read by computer programs or other forms of media" are protected. Because the law provides circumstances in which temporary reproductions are not considered infringement, it appears to implicitly accept that some temporary reproductions are considered infringement. Importantly, the law now provides prohibitions against the circumvention of technological protection measures (TPMs), including both access controls and copy controls. However, the law does not include clear provisions prohibiting trafficking in devices, technologies, and services primarily designed to circumvent TPMs. The copyright law doubles criminal penalties for copyright infringement.

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**.

[104] 2018 BSA Global Software Survey, *op. cit.*

[105] *Copyright Law of Indonesia* (2014) at: https://wipolex.wipo.int/en/text/369562

VIETNAM

Due to extremely high levels of unlicensed software use by enterprises and government institutions, the lack of criminal enforcement against willful 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 online services in Vietnam.[106] 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.[107]

BSA receives good 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.[108]

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 Ministry of Public Security (MPS) issued draft implementing measures for stakeholder input with a deadline of January 2, 2019 for submitting comments.[109]

The Law raises serious concerns and will likely significantly impact the ability of many BSA members to provide software products and services in Vietnam. Specifically, the law requires data to be stored in Vietnam, requires all service providers to have a local presence in Vietnam, and grants authorities the ability to restrict international data transfers and require the disclosure of content in unencrypted form. The breadth of the Law far exceeds cybersecurity protection and extends to a broad regulation of the Internet generally. 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.

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.

---

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

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

[108] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at: 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.

[109] BSA Comments on the Draft Decree Implementing Law on Cybersecurity at: https://www.bsa.org/~/media/Files/Policy/Data/12142018BSA_Position_Paper_on_Draft_Decree_implementing_Law_on_Cybersecurity_%20ENG.pdf

Information Security: The National Assembly enacted the Law on Network Information Security (LONIS) on November 19, 2015.[110] 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 unclear how the LONIS and the Cybersecurity Law will interact, raising additional uncertainty and compliance costs for BSA members.

Cross-Border Data Flows and Server Localization: On September 1, 2013, Decree No. 72 went into effect.[111] 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.[112]

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.

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code,[113] the Criminal Code,[114] and the Administrative Violations Decree.[115] The Civil Code operates in parallel.[116]

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. Further, while Article 170a of the current Criminal Code improves Vietnam's statutory framework in some respects, it is now weaker than previous provisions found in the February 2008 Criminal

[110] *Law on Network Information Security (LONIS)* (2018). English translation at: http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf

[111] *Decree No. 72 72/2013/ND-CP on the Management, Provision, and Use of Internet Services and Online Information.* English translation at: https://vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF

[112] 2018 BSA Global Software Survey, *op. cit.*

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

[114] *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

[115] *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.

[116] *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

Circular.[117] The lack of criminal enforcement against copyright infringement over the years is also due to the fact that the Criminal Code only applies to natural persons, not to entities.

On January 1, 2018, amendments to Vietnam's Criminal Code (adopted in 2015) went into effect.[118] 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.

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 willful 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**.

[117] The 2008 Circular criminalized all acts of "infringement" by referring to Articles 28 and 35 of the Intellectual Property Code, including all acts of infringement defined therein, as well as violations involving circumvention of technological protection measures, decryption of encrypted satellite signals, and other acts.

[118] *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

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 effective laws on cybercrime and electronic signatures. However, Argentina still restricts cross-border data transfers and maintains other measures that negatively affect the digital economy. The country 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 and technology neutral and nondiscriminatory government procurement of information technology (IT).

Market Access

The requirements for cross-border transfers in Argentina are complex and subject to a range of restrictions, as reflected in Regulation No. 60-E/2016, issued by the National Commission for the Protection of Personal Data (Dirección Nacional de Protección de Datos Personales (DNPDP)) in November 2016. Argentina's cross-border data transfer provisions include cumbersome registration requirements and mandatory contractual clauses.

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.[119]

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 manufacture 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 intellectual property (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 in particular, the software industry continues to seek from the Under Secretariat for Public Administration (the Subsecretaría de la Gestión Pública) 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.

Recommended reforms to Argentine copyright law include: (1) extending the scope of reproduction rights to explicitly cover temporary copies; (2) protecting against the act of circumvention, as well as the manufacture or distribution of devices aimed at circumventing technological protection measures (TPMs); (3) establishing

[119] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at: 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.

effective statutory damage provisions in civil infringement cases; (4) establishing a statutory framework of "safe harbor" protections for intermediaries; and (5) recognizing 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

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

On the other hand, the environment for IP protection and enforcement has generally improved in Brazil, with BSA and its members enjoying cooperation with law enforcement and working within a generally satisfactory judicial system. More remains to be done, however, to improve efficiency and reduce the costs of IP enforcement, and to bring down the high rates of unlicensed software use.

Market Access

A variety of existing and proposed measures related to privacy and public procurement preferences have created, or threaten to 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 barriers to foreign software. This situation may, paradoxically, increase risks of security vulnerabilities and decrease the confidence of Brazilian consumers that their sensitive personal data will be appropriately protected.

Privacy Legislation*:* After more than four years of discussion, in July 2018 the Brazilian Congress approved the Data Privacy Bill. The Bill was signed into law by the President in August 2018. Following this, in December 2018, the Executive branch issued a Provisional Measure creating the Data Protection Authority (DPA). The main responsibilities of DPA are to: (1) interpret the Data Privacy Bill and apply fines regarding data protection; (2) enact data protection norms and procedures; and (3) foster the cooperation with foreign data protection authorities. The decisions from DPA will supersede all others by government agencies regarding data protection in Brazil. The Provisional Measure will be reviewed by Congress through June 2019. After review, the President would be able to sign it into law. Ensuring proper implementation of the law will be key to avoid any adverse impact on US companies operating in the Brazilian market.

Data and Server Localization Requirements: The Guidelines on Government Procurement of Cloud Services were issued in draft format in 2017 and are currently pending. If finalized and implemented as drafted, the guidelines will create server and data localization requirements that will negatively impact procurement of cloud computing services by all Federal agencies. BSA submitted comments on the draft guidelines urging the Government of Brazil to remove the localization requirements but, unfortunately, there are no indications that the regulation will be modified to address this issue.[120] BSA urges the US government to establish a dialogue with the Bolsonaro Administration to demonstrate the importance of the elimination of data localization requirements.

Government Procurement Barriers*:* Presidential Decree 8135/2013 (Decree 8135) regulates the use of IT services provided to the Federal government by private and state-owned companies, including the provision that Federal IT communications be hosted by Federal IT agencies. In 2015, the Ministry of Planning developed regulations to implement Decree 8135, which include: (1) technical specifications for standardized services; (2) contract rules, conditions, and prices; (3) interoperability standards; (4) management of agency solicitation of services; and (5) periodic price review. The regulations present serious challenges for BSA members, including the deviation from global standards and requirements to disclose source code and other IP. In 2016, the Federal government announced it would revoke Decree

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

8135. A new decree was expected to be published by the end of 2016, but the new decree is still pending to this date. The new decree and implementing regulations should allow Federal agencies to procure innovative IT products and services, including cloud computing, and avoid restrictive data localization policies.

Government Procurement Preferences*:* Presidential Decree 8186/2014 establishes an 18 percent price preference for local products and guidelines for the following categories: software licenses, software application development services (customized and un-customized), and maintenance contracts for applications and programs. Public procurement preferences for local products and services, as well as technologies developed in Brazil, would also be required by the pending Guidelines on Government Procurement of Cloud Services, which was published in draft format in early 2017.

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

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.[121] This is a far greater value of unlicensed commercial software than what has been measured throughout the rest of the region. Although recent 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.

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 software asset management (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 the use of unlicensed software.

BSA's relationship with the enforcement authorities in the past year 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

[121] 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.

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 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**.

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. The rate of unlicensed software in Mexico is 49 percent, representing an estimated commercial value of US$760 million in unlicensed software.[122] 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 an ongoing effort for all governments. 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 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 in Mexico, once this agreement is ratified by the Mexican Senate.

While it is positive that IMPI has appointed law enforcement officers in all of its regional offices (Guadajara, Monterrey, Mérida, León, and Puebla) and 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 administrative and 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.

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.

Consistent with the provisions of the USMCA, Mexico should also ensure that adequate enforcement procedures and legal remedies are available for right holders to address copyright infringement online, i.e. 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 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

[122] 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.

decision in the Amparo 1/2017 is still being used by ISPs as an argument to not fully cooperate with rights holders.

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. PGR's experts lack sufficient knowledge, training, and expertise to deal with digital copyright issues. This is a good time to carefully consider and implement change because the criminal system is currently undergoing a transition. The delay caused by the change in administration and corresponding prosecution of IP related crimes poses another crucial challenge.

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.[123]

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

[123] In 2017, 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 Mexican Attorney General's Office (PGR), customs inspectors, inspectors from the Federal Consumer Protection Commission (PROFECO), judges, certified public accountants, industry association members, police officers, entrepreneurs, students, importers, and exporters. The programs covered a broad range of IP and innovation-related topics including IP rights and software protection, artificial inteligence, big data, the Internet of Things, cloud computing, privacy, innovation, cybersecurity, ISP liability, copyright infringement and damages, software-related tax matters, customs enforcement, licensing, administrative practices, notorious markets, and rule of law, among others. BSA carried out these activities in collaboration with various educational institutions, the Mexican Institute of Public Accountants, chambers of commerce, and associations. BSA also woked with think tanks including the Coalition for the Legal Access to Culture and Mexico Exponencial, 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.

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.[124] 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 came into force on September 28, 2015 it remains difficult to provide cloud-based services to the Korean market.[125] Data residency, physical network separation, and other requirements for sectors, such as government/public services, finance, healthcare, and education, hamper the ability to provide cloud-based services to users in these sectors.

The Government of Korea is actively developing its policies for moving Korea ahead in the digital economy. In 2017, the Administration established the Presidential Committee on the Fourth Industrial Revolution, now in its second term, to formulate and implement a strategic plan for this purpose.[126] 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).[127] 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 members in Korea. These especially affect those providing Internet-enabled services, such as cloud-computing and data analytics services.

Cross-Border Data Flows and Server Localization: Although the Cloud Computing Promotion Act came into force on September 28, 2015, it remains very difficult for commercial cloud services providers (CSPs)

---

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

[125] *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

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

[127] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at: 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.

to offer cloud services to entities in Korea's very broadly defined public sector.[128] This is due to onerous certification requirements imposed by the Korea Internet Security Agency (KISA) on CSPs who provide cloud services to public sector agencies and requirements for physical network separation. Similar guidelines and regulations requiring physical network separation or data on-shoring apply to the finance and healthcare sectors.[129] 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., finance and healthcare) from adopting commercial cloud computing and related services.

The Regulation on Supervision of Electronic Financial Transactions (RSEFT)[130] was amended on October 5, 2016 to permit the use of cloud services by financial services institutions (FSIs). The amendment allows certain data to be stored on public cloud services. FSC recently approved the use of personal credit information by public cloud services and may be considering additional measures to expand the ability to manage financial data on the public cloud. However, FSC specifically requires that such data be maintained on servers located in Korea.[131]

Personal Information Protection Regime: Korea's personal information protection (PIP) regime is one of the most stringent in the region and has significantly decreased the ability for BSA members to serve the Korean market. The two relevant pieces of legislation are the Personal Information Protection Act (PIPA)[132] and the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act).[133]

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

In November 2018, the government proposed amendments to the Network Act, PIPA, and the Credit Information and Protection Act.[134] If enacted, these amendments would provide a legal basis for use of pseudonymous information without the consent of the provider. Also, the National Assembly proposed bills

---

[128] Cloud Computing Promotion Act, *op. cit.*

[129] 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;"

[130] *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

[131] 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.

[132] *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

[133] *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

[134] *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

to separate the Personal Information Protection Commission (PIPC) from the Ministry of Interior and Security (MOIS) and transfer personal information related clauses from the Network Act to the PIPA. The amended PIPA would then be governed by the Commission.

Unfortunately, even with these improvements, Korea's PIP regime would continue to impose onerous and prescriptive obligations, many of which restrict cross-border transfers of personal information that are necessary for overseas-based service providers to serve the Korean market.

On August 29, 2018 the National Assembly passed a Bill amending the Network Act.[135] The Bill 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: The Ministry of Science and ICT (MSIT) enacted the Guideline of IT Network Equipment Installations in Public Sector (Guideline)[136] in 2017 to give preference to domestic small and medium-sized enterprises (SMEs). The Guideline significantly limits US suppliers access to many public sector procurement opportunities and they are inconsistent with Korea's international commitments. In 2018, MSIT proceeded to propose amendments to the Special Act on Promotion of Information and Communications Technology, Vitalization of Convergence Thereof, Etc. (ICT Special Act)[137] to provide a firmer legal basis for the Guideline. MSIT, in the explanatory note of the proposed legislative amendment,[138] 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.[139] 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."[140] 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.

---

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

[136] 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

[137] 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

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

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

[140] *Ibid.*

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.

Copyright and Enforcement

The rate of unlicensed software use in Korea has continued a slow, steady decline. According to the latest data, 32 percent of software used in Korea in 2017 was unlicensed, which equates to a market value of US$598 million in unlicensed software.[141] While this figure is below the regional and global average for unlicensed software use, it remains relatively high compared to similar economies in the region and around the world. BSA acknowledges and supports the Government of Korea's goal to reduce the rate of unlicensed software use to less than 30 percent by 2020.

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 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 to less than 30 percent by 2020, 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. In 2019, Korea should amend the Civil Procedure Act, as the Supreme Court of Korea has suggested, to include effective discovery rules in civil cases.[142]

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**.

[141] 2018 BSA Global Software Survey, *op. cit.*

[142] *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

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 under consideration — one on cybersecurity protection of critical infrastructure, and the other on personal data protection — are important elements of this effort. BSA agrees that it is important for Thailand to enact robust and effective cybersecurity and personal data protection legislation. However, we remain concerned that both bills, as currently drafted, could undermine the RTGs efforts to enhance cybersecurity and personal data protection, interfere with the government's broader goals to drive Thailand 4.0, and unfairly impede BSA member companies' ability to effectively provide products and services to the Thai market.[143]

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

Market Access

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

Security: Thailand's 2015 National Cybersecurity Bill was designed to strengthen the cybersecurity capabilities of government agencies and provide appropriate breach notification procedures. However, the bill raised concerns because it gave the National Cybersecurity Committee (NCSC) broad powers to access confidential and sensitive information without sufficient protections, such as opportunities to appeal or limit such access. In our 2015 comments, BSA highlighted that granting the NCSC such broad powers would undermine public confidence and trust in information technology (IT) generally and harm the ability of BSA members to provide the most innovative and effective software solutions and services to the market in Thailand.[144]

In April and May 2018, BSA (along with the US-ASEAN Business Council) submitted comments to Thailand's Ministry of Digital Economy and Society (MDES) on the 2018 version of the National Cybersecurity Bill.[145] BSA's chief concerns center around: the composition of the NCSC, the broad powers of the NCSC, the notification regime for cyber-attacks, surveillance authority, and criminal liability.

In September, MDES released another, purportedly near final, version of the National Cybersecurity Bill, upon which BSA filed another set of comments, focusing on similar concerns that we have described in the past.[146] The Bill was introduced to the National Legislative Assembly (NLA) on December 28 and passed

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

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

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

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

the first reading. We understand that a Committee is set to debate the Bill during the second reading within 45-60 days of the first reading.

Privacy: The Personal Data Protection Bill (PDP Bill) was also introduced to the NLA on December 28 and is under review by the same Committee. 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.[147] The most recent version also heavily draws from the recently implemented General Data Protection Regulation (GDPR) of the European Union.

Since 2015, when we first submitted comments on Thailand's PDP Bill, BSA has highlighted the importance of protecting personal information to foster the trust and confidence necessary to grow the digital economy.[148]

In our most recent comments to MDES on the January 2018 version of the PDP Bill, BSA noted the significant improvements over earlier drafts and proposed recommendations on several provisions that still threaten to create unreasonable burdens and legal uncertainty for the technology sector.[149] BSA's chief concerns relate to unclear or unreasonable obligations on personal data processors, the still too limited legal bases for handling personal data, potential impediments to international data transfers, certain elements of the data breach notification system, and the scope and limits of the powers of the Personal Data Protection Committee (PDPC) and Expert Committees.

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

Copyright and Enforcement

BSA enjoyed very good cooperation with RTG authorities in 2018, including with the Economic Crime 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.[150]

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.[151] BSA urges the RTG to adopt 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

---

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

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

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

[150] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at: 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.

[151] "*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).

improved the effectiveness of IP litigation in Thailand. Unfortunately, although 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, by 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 2018 included the Department of Intellectual Property (DIP), the Department of International Trade Promotion's New Economy Academy (NEA), the ECD, the Central Intellectual Property and International Trade Court, the Securities and Exchange Commission, the MDES, and the Electronic Transactions Development Agency. BSA worked with the SEC to organize a series of events to educate SEC listed companies on the benefits of SAM, as well as with the DIP and the NEA to educate startups, small- and medium-sized businesses, and other private enterprises.

Technical Assistance and Education: In 2018, BSA, the DIP, the ECD, and the NEA continued the joint national campaign "Safe Software, Safe Nation" to promote the use of licensed software. The campaign also explains the security risks posed by unlicensed software. BSA continued to promote software asset management (SAM) practices based on International Standards Organization (ISO) standards, reaching over 5,000 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 security-related legislation now pending 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

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

Market Access

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

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 from any other market including key markets such as China, South Korea, and Russia.

The US-EU Privacy Shield, which replaced the former Safe Harbor framework for data transfers from Europe to the United States, took effect on August 1, 2016, and represents a strong agreement to foster transatlantic data transfers while safeguarding consumer privacy. Despite two successful Annual reviews (in 2017 and 2018), where the European Commission concluded that this framework continues to ensure adequate protection and safeguards for personal data transferred from the EU to the United States, it was immediately challenged before the European Court of Justice (ECJ) in cases brought by two privacy activist groups (Digital Rights Ireland and La Quadrature du Net). While Digital Rights Ireland's challenge has been dismissed, the General Court is looking at the merits of the second challenge. The written procedure on the second case was closed December 4, 2018 and referred to the "extended format" of the second Chamber of the Court, with a hearing and a decision on the case expected for late 2019. These groups contend that US practices on law enforcement and national security access to data lack sufficient privacy safeguards, and as such, the Privacy Shield should be invalidated. These legal challenges mean US companies will face continuing uncertainty in relying on the Privacy Shield for transatlantic data transfers.

In May 2016, the Irish Data Protection Commissioner requested that the Irish High Court ask the Court of Justice of the European Union ("CJEU") to examine whether Standard Contractual Clauses ("SCCs") violate EU citizens' fundamental rights insofar as there is insufficient judicial redress for EU citizens when their data is transferred to third countries, such as the 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. A decision on the case is expected in late 2019.

Data Flows in Trade Agreements with Third Countries: In February 2018, the European Commission released a draft text on data flows in trade agreements, seeking to address concerns from Member States,

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

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

Proposed e-Privacy Regulation: In January 2017, the European Commission published a Regulation aiming to update the EU's current e-Privacy Regulation (ePR), which regulates the confidentiality of communications and processing of personal data on terminal equipment. The scope of the proposed regulation is very broad, sweeping in any electronic communications service provided with the use of a public communications network, including over-the-top services and machine-to-machine communications (e.g., data transfers between Internet of Things devices). It also would apply extraterritorially, including in circumstances where processing is conducted outside the EU in connection with services provided within the EU. The draft Regulation built around a consent-only processing model, risks contradicting key provisions of the General Data Protection Regulation ("GDPR"). BSA submitted comments, expressing concern for the wide-reaching and prescriptive rules included in the ePR and the narrow number of exceptions.[152]

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

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

Intellectual Property

Text Data and Mining: In September 2016, the European Commission proposed new copyright rules which create a specific, but narrow exception to perform text and data mining ("TDM") for non-public interest research organizations. In May 2018, the Council reached its position on the draft Directive. The European Parliament is in the process of adopting its position on the proposed Copyright Directive. In July 2018, the European Parliament rejected the initial report on the draft Directive. In September 2018, the European Parliament endorsed the European Parliament's Committee on Legal Affairs (JURI) draft

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

Report, and on October 2, the “trilogues” between the European Commission, European Parliament, and Council started, with the aim to finalize discussions prior to the 2019 European elections. The final text is expected to allow Member States to enact an optional national exception for all actors engaging in reproductions and extractions of lawfully accessible works that form part of the process of TDM. To the extent that certain Member States do not implement such a national exception, the ability of BSA members to perform TDM may be undermined, resulting in barriers to digital trade in those countries.

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.**

Selected BSA Resources

Artificial Intelligence

AI Policy Overview (2018)
www.bsa.org/~/media/Files/Policy/BSA_2018_AI_PolicyOverview.pdf

Building Confidence and Trust in Artificial Intelligence Systems (May 2018)
https://ai.bsa.org/wp-content/uploads/2018/05/BSA_2018_AI_Accountability.pdf

Understanding AI (2017)
www.bsa.org/~/media/Files/Policy/BSA_2017UnderstandingAI.pdf

Spurring AI Innovation with Sound Data Policy (May 2018)
ai.bsa.org/wp-content/uploads/2018/05/BSA_2018_AI_DataPolicy.pdf

Encryption

Critical Infrastructure Cybersecurity Depends Upon Strong Encryption (2018)
www.bsa.org/~/media/Files/Policy/Data/BSA_Encrypt_CriticalInfrastructure-web.pdf

Encryption is a Critical Safeguard Against Data Breaches (2018)
www.bsa.org/~/media/Files/Policy/Data/BSA_Encrypt_DataBreach-web.pdf

More Data is Available to Law Enforcement Than Ever Before (2018)
www.bsa.org/~/media/Files/Policy/Data/BSA_Encrypt_AvailabilityData-web.pdf

Strong Encryption Has Measurably Improved Device Security (2018)
www.bsa.org/~/media/Files/Policy/Data/BSA_Encrypt_DeviceSecurity-web.pdf

Data Privacy and Security

BSA Cybersecurity Agenda (April 2018)
https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_CybersecurityAgenda.pdf

BSA International Cybersecurity Policy Framework (2018)
https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf

BSA Privacy Framework (2018)
www.bsa.org/~/media/Files/Policy/BSA_2018_PrivacyFramework.pdf

Global Privacy Best Practices (2018)
www.bsa.org/~/media/Files/Policy/Data/2018_BSA_Global_Privacy_Best_Practices.pdf

Strengthening Cybersecurity Through Value-based IT Procurement (Feb. 2018)
https://www.bsa.org/~/media/Files/Policy/Security/General/BSA_LPTA%20One-Pager_021518.pdf

Trade and Global Markets

BSA Digital Trade Agenda - Modernizing Digital Trade: An Agenda for Software (May 2017)
www.bsa.org/~/media/Files/Policy/Trade/05222017BSANAFTAHandoutPress.PDF

Cross-Border Data Flows (2017)
www.bsa.org/~/media/Files/Policy/BSA_2017CrossBorderDataFlows.pdf

Global Cloud Computing Scorecard (2018)
cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf

Other

BSA Policy Agenda (2019)
www.bsa.org/~/media/Files/Policy/BSA_2019USPolicyAgenda.pdf

BSA Workforce Development Agenda (May 2018)
www.bsa.org/~/media/Files/Policy/workforce/05022018BSAWorkforceDevelopmentAgenda.pdf

Global Software Survey (2018)
www.bsa.org/globalstudy

Global Software Survey (2016)
globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf

Unlicensed Software and Cybersecurity Threats Whitepaper (2015)
globalstudy.bsa.org/2013/Malware/study_malware_en.pdf

What is the Big Deal with Data (Dec. 2015)
data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf.

International Trade- and IP-Related Submissions to the US Government

Letter to USTR Ambassadors Jeffrey D. Gerrish and C.J. Mahoney regarding United States – Japan Trade Negotiations (Oct. 2018)
www.bsa.org/~/media/Files/Policy/Trade/10122018US_JP_DigitalTradeLetter.pdf

Letter to USTR Ambassador Robert E. Lighthizer regarding NAFTA Negotiations (May 2018)
www.bsa.org/~/media/Files/Policy/Trade/05142018BSALetterAmbassadorLighthizerNAFTA.pdf

Submission to the Office of the US Trade Representative, *US-UK Trade Negotiations*, USTR-2018-0035 (Jan. 2019)
www.bsa.org/~/media/Files/Policy/Trade/en01152019BSAUSUKComments.pdf

Submission to the Office of the US Trade Representative, *Negotiating Objectives for a United States – European Union Trade Agreement*, USTR-2018-0035 (Dec. 2018)
www.bsa.org/~/media/Files/Policy/Trade/12072018BSAUSEUtradecomments.pdf

Submission to the Office of the US Trade Representative, *Negotiating Objectives for a United States – Japan Trade Agreement*, USTR-2018-0034 (Nov. 2018)
www.bsa.org/~/media/Files/Policy/Trade/11262018BSA_US_JapanCommentsTradeAgreement.pdf

Submission to the Office of the US Trade Representative, *National Trade Estimate Report on Foreign Trade Barriers,* USTR-2018-0029 (Oct. 2018)
www.bsa.org/~/media/Files/Policy/Trade/10302018BSANTESubmission.pdf

Submission to the Office of the US Trade Representative, *NAFTA Negotiations* (June 2017)
www.bsa.org/~/media/Files/Policy/Trade/06122017_BSANAFTAComments.pdf

Testimony before the Office of the US Trade Representative, *Negotiating Objectives for US-UK Trade Agreement* (Jan. 2019)
www.bsa.org/~/media/Files/Policy/Trade/01292019JosephWhitlockUSUKTestimony.pdf

Testimony before the U.S. International Trade Commission, *United States-Mexico-Canada Agreement - Likely Impact on the US Economy and on Specific Industry Sectors*, Inv. No. TPA-105-003 (Oct. 2018)
www.bsa.org/~/media/Files/Policy/Trade/10302018USMCAHearingStatement.pdf

Testimony before the Office of the US Trade Representative, *NAFTA Negotiations* (June 2017)
www.bsa.org/~/media/Files/Policy/Trade/06252017NAFTANegotiationsHearingRemarks.pdf

Written Statement to US International Trade Commission, *Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions,* Inv. No. 332-TA-561 (2017)

Country-Specific Resources

Argentina

Cloud Scorecard – Argentina Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Argentina.pdf

Brazil

Cloud Scorecard – Brazil Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Brazil.pdf

Submission on the Brazilian Central Bank's Proposed Regulation on Cybersecurity Policies and the Procurement of Data Processing, Data Storage, and Other Cloud Computing Services, Public Consultation 57/2017 (Nov. 2017)
www.bsa.org/~/media/Files/Policy/Data/11212017CommentsonCentralBankRegulations_English.pdf

Submission on Public Procurement of Cloud Computing Services Draft Guidelines (March 2017)
https://www.bsa.org/~/media/Files/Policy/Filings/CommentsBSA_CloudProcurement.pdf

China[153]

Cloud Scorecard – China Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/press_releases/China_pr_en.pdf

Submission to the Office of the US Trade Representative, *Proposed Modification of Action Pursuant to Section 301 - China's Acts, Policies and Practices Relating to Technology Transfer, Intellectual Property, and Innovation*, USTR-2018-0026 (Sept. 2018)
www.bsa.org/~/media/Files/Policy/Trade/09052018BSASection301Letter.pdf

Submission to the Ministry of Public Security, *Cybersecurity Classified Protection Regulations* (Aug. 2018)
www.bsa.org/~/media/Files/Policy/Data/08082018USITOCommentsDraftCybersecurityClassifiedProtectionRegulationsEN.pdf

Submission to the Office of the US Trade Representative, *Proposed Determination of Action Pursuant to Section 301, China's Acts, Policies and Practices Relating to Technology Transfer, Intellectual Property, and Innovation*, USTR-2018-0005 (May 2018)
www.bsa.org/~/media/Files/Policy/Trade/05112018BSACommentsChinaProductTariffList.pdf

Submission to the Office of the US Trade Representative, *China's Acts, Policies and Practices Relating to Technology Transfer, Intellectual Property, and Innovation*, USTR-2017-0016 (Sept. 2017)
www.bsa.org/~/media/Files/Policy/Trade/09282017BSAUSTR301CommentsChina.pdf

[153] As a member of the United States Information Technology Office (USITO), BSA makes most of its submissions to the Chinese government under the auspices of USITO.

European Union

EU ePrivacy Regulation Position Paper (2017)
www.bsa.org/~/media/Files/Policy/Data/09202017BSAPositionPaperontheEUePrivacyRegulation.pdf

Why is Data Leaving the EU an Issue for US Businesses? (Sept. 2018)
www.bsa.org/~/media/Files/Policy/Trade/09182018BSAPrivacyShield.pdf

Letter to the Council for the European Union, *Policy Debate on the Progress of Negotiations on the draft ePrivacy Regulation* (June 2018)
www.bsa.org/~/media/Files/Policy/Data/06052018BSALetter_ePrivacy_Regulation_TTECouncil.pdf

France

Cloud Scorecard – France Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_France.pdf

Germany

Cloud Scorecard – Germany Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Germany.pdf

India

Cloud Scorecard – India Country Report (2018)
cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf

Submission to Telecom Regulatory Authority of India, Consultation Paper on Regulatory Framework for Over-The-Top (OTT) Communication Services (Jan. 2019)
www.bsa.org/~/media/Files/Policy/Data/01072019BSASubmissionTRAIonOTTConsultation.pdf

Submission regarding India Personal Data Protection Bill (Sept. 2018)
https://www.bsa.org/~/media/Files/Policy/Data/09282018BSACommentsonIndiaDataProtectionBill.pdf

Submission to Reserve Bank of India, *Directive on Storage of Payment Systems Data* (June 2018)
www.bsa.org/~/media/Files/Policy/Data/06222018BSASubmissiontoReserveBankofIndia.pdf

Submission regarding *White Paper of the Committee of Experts on a Data Protection Framework for India* (Jan. 2018)
www.bsa.org/~/media/Files/Policy/Data/012918BSAResponseofWhitePaperDataPortectionFrameworkIndia.pdf

Submission regarding *Draft Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products* (Oct. 2017)
www.bsa.org/~/media/Files/Policy/Data/10262017BSACommentsonIndiaMEITY DraftCyberSecurityProductsNotification.pdf

Submission to Telecom Regulatory Authority of India, *Recommendations on Privacy* (Oct. 2017)
https://www.bsa.org/~/media/Files/Policy/Data/10302017BSACommentsonIndiaTRAIConsultationonPrivacySecurityandOwnerhipoftheDataintheTelecomSector.PDF

Submission to Telecom Regulatory Authority of India, *Cloud Computing Consultation Paper* (July 2016)
https://www.bsa.org/~/media/Files/Policy/Data/07252016BSASubmissiononCloudComputingIndia.pdf

Indonesia

BSA Cloud Scorecard – Indonesia Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Indonesia.pdf

Submission to Ministry of Communication and Information Technology, *Draft Amendments to GR82* (March 2018)
https://www.bsa.org/~/media/Files/Policy/Data/03012018BSAJointSubmissionOnGR82Amendment.pdf

Italy

BSA Cloud Scorecard – Italy Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Italy.pdf

Mexico

BSA Global Software Survey – Mexico Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Mexico.pdf

Poland

Cloud Scorecard – Poland Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Poland.pdf

South Korea

BSA Cloud Scorecard – Korea Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Korea.pdf

Letter to the National Assembly, Request to Postpone Amendments to Article 19(3) of Framework Act on Consumers Pending Consultation with Affected Stakeholders (Nov. 2018)
www.bsa.org/~/media/Files/Policy/Data/en11222018LetterROKreConsumerAmendments.pdf

Submission regarding *Proposed Amendments to the Network Act and to the Telecommunications Business Act* (Nov. 2018)
www.bsa.org/~/media/Files/Policy/Data/en11292018BSASubmissionAMCHAMPositionPaperBJIKKJ.pdf

Submission to Korea Ministry of Trade Industry and Energy on the United States-Korea Free Trade Agreement Renegotiation (Nov. 2017)
www.bsa.org/~/media/Files/Policy/Trade/11242017BSASubmissiononKORUSFTA.pdf

Spain

BSA Cloud Scorecard – Spain Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Spain.pdf

Thailand

BSA Cloud Scorecard – Thailand Country Report (2018)
https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Thailand.pdf

Submission to National Assembly of Thailand, *Personal Data Protection Bill and National Cybersecurity Bill* (Jan. 2019)
www.bsa.org/~/media/Files/Policy/Data/01312019BSASubmissionNLACommittee.pdf

Submission to Ministry of Digital Economy and Society, *Thai National Cybersecurity Bill* (Nov. 2018)
www.bsa.org/~/media/Files/Policy/Data/en11302018BSACommentsCybersecurityBill15November2018.pdf

Submission to Ministry of Digital Economy and Society, *Thai National Cybersecurity Bill* (Oct. 2018)
www.bsa.org/~/media/Files/Policy/Data/10122018EN_BSACommentsCybersecurityBillwith%20Annexes.pdf

Submission to the Ministry of Digital Economy and Society, *Cybersecurity Bill – Supplemental* (May 2018)
www.bsa.org/~/media/Files/Policy/Data/05252018BSAComments_PPC_SupplementaryRules.PDF

Submission to the Ministry of Digital Economy and Society, *Cybersecurity Bill* (April 2018)
www.bsa.org/~/media/Files/Policy/Data/04172018JointBSA_USABC_Comments_on_Thai_Cybersecurity_Bill.pdf

Submission on Thailand Copyright Directive (March 2018)
www.bsa.org/policy/~/media/Files/Policy/IntellectualProperty/03092018BSACommentsThailandCopyrightAmendmentBill.pdf

Submission to the Ministry of Digital Economy and Society, *Draft Personal Data Protection Act* (Feb. 2018)
www.bsa.org/~/media/Files/Policy/Data/02062018BSASubmissionThaiPersonalDataProtectionBill.pdf

Turkey

BSA Cloud Scorecard – Turkey Country Report (2018)
cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Turkey.pdf

Vietnam

BSA Cloud Scorecard –Vietnam Country Report (2018)
cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Vietnam.pdf

Submission to the Ministry of Public Security, *Draft Decree Implementing the Law on Cybersecurity* (Dec. 2018)
www.bsa.org/~/media/Files/Policy/Data/12142018BSA_Position_Paper_on_Draft_Decree_implementing_Law_on_Cybersecurity_%20ENG.pdf

Submission to the National Assembly of Vietnam, *Joint Industry Comments on May 24 Revised Draft law on Cybersecurity* (June 2018)
www.bsa.org/~/media/Files/Policy/Data/06052018VNJointIndustrySubmissiondraftCybersecLaw.pdf

Submission to the Ministry of Public Security, *Joint Industry Comments on Draft Law on Cybersecurity* (Feb. 2018)
www.bsa.org/~/media/Files/Policy/Data/02262018BSAJointIndustry%20CommentsVietnamCybersecurityLaw.pdf

United Kingdom

Submission to the United Kingdom Department of International Trade, *Consultation on Trade Negotiations with European Union* (Dec.2018)
https://www.bsa.org/~/media/Files/Policy/Trade/12072018BSAUSEUtradecomments.pdf

Submission to the United Kingdom Department of International Trade, *Consultation on Accession to the CPTPP* (Oct. 2018)
https://www.bsa.org/~/media/Files/Policy/Trade/10262018BSASubmissionUKConsultationtojoinCPTPPOctober2018.pdf

Submission to the United Kingdom Department of International Trade, *Consultation on Trade Negotiations with Australia* (Oct. 2018)
https://www.bsa.org/~/media/Files/Policy/Trade/10262018BSASubmissionUKConsultationwithAustralia.pdf

Submission to the United Kingdom Department of International Trade, *Consultation on Trade Negotiations with New Zealand* (Oct. 2018)
https://www.bsa.org/~/media/Files/Policy/Trade/10262018BSACommentsUKConsultationwithNewZealand.pdf

Submission to the United Kingdom Department of International Trade, *Consultation on Trade Negotiations with the United States* (Oct. 2018)
www.bsa.org/~/media/Files/Policy/Trade/10262018BSACommentsUKConsultationwithUnitedStates.pdf

Selected Software.org Resources

Artificial Intelligence – Maximizing the Benefits (2018)
software.org/wp-content/uploads/AI_Report.pdf

Blockchain Primer: From Enabling Bitcoin to Blocking Blood Diamonds (2017)
software.org/reports/blockchainprimer/

Brazil 4.0 - The Data-Driven Future of Brazilian Industries (2018)
software.org/wp-content/uploads/Software_Brazil4.0_English.pdf

Encryption's Vital Role in Industrial Control Systems (2018)
software.org/wp-content/uploads/Software_ICS_Encryption.pdf

Every Sector Is a Software Sector: Manufacturing, How Software Is Turbocharging Manufacturing Opportunities for All (2018)
software.org/wp-content/uploads/Every_Sector_Software_Manufacturing.pdf

Infrastructure 4.0: Rebuilding America with Software (2018)
https://software.org/wp-content/uploads/Infrastructure-4-0.pdf

Sensor Sensibility: Getting the Most from the Internet-of-Things (2017)
https://software.org/wp-content/uploads/iot-sensor-sensibility.pdf

The Growing $1 Trillion Economic Impact of Software (2017)
software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf

The Growing €1 Trillion Economic Impact of Software (2018)
software.org/wp-content/uploads/2018_EU_Software_Impact_Report_A4.pdf